The Open University
BUSINESS SCHOOL

LESSONS FROM PRACTICE: INSIGHTS ON CYBERSECURITY STRATEGY FOR BUSINESS LEADERS, FROM SMES TO GLOBAL ENTERPRISES

James Crotty and Professor Elizabeth Daniel

FOREWORD

As the use of electronic data and online networks becomes more pervasive across society and within businesses and institutions, so too does the threat to our cybersecurity. For us to benefit from the extraordinary technological developments we have seen in data and online access over the past two decades, it is essential for all of us – businesses, institutions and individuals – to understand the nature of the danger posed by this pernicious cyber threat, and the practical steps we can all take to mitigate against this. While there is no such thing as 100 percent security in cyberspace, there are things we all can and must do to enhance our security in this arena.

Responding to the needs of individuals and employers and the communities in which they live and work is critical to The Open University Business School. Our aspiration, along with that of the wider University, is to foster the conduct of applied research to address real world problems. This report achieves those aims by sharing practical insights into the development of a cybersecurity strategy for organisations, from SMEs to global operators. I am therefore delighted to have the opportunity to write this foreword and recommend the report to you as a business leader or individual.

The report brings together insights and recommendations on the development of cybersecurity capabilities from risk and cybersecurity practitioners based within some of the world's foremost organisations. Also, reflecting the reality that cybersecurity is not just an IT issue but an organisational challenge that must be owned by business leaders, the report has been reviewed by an array of our business and technology academics.

All of the industry practitioners and academic reviewers who have contributed to this report have been incredibly generous with their time and invaluable insights. For this, the authors and The Open University Business School are most grateful.

Professor Devendra Kodwani

Executive Dean, Faculty of Business and Law
The Open University

EXECUTIVE SUMMARY

This paper is based on interviews with industry-leading cybersecurity and risk practitioners and the findings of an extensive literature review. It provides an insight into the extent of the cyber threat organisations are facing today and offers recommendations for business leaders in organisations of all sizes on practical steps they can take to develop a cybersecurity strategy.

Cyber threat is a real and present danger for enterprises of every size and sector that engage in any form of electronic data exchange: some hope for security in obscurity but this is a false hope. Knowingly or unknowingly, organisations are becoming significant data stewards in an age of exponential data growth. Cybersecurity failures perpetrated by malicious actors or human error are a threat every organisation must take steps to address. Boards and other business leaders have a responsibility to all of their enterprise stakeholders to do so.

In response to the pervasive and growing cybersecurity challenge a vast array of frameworks and guidelines have been proposed by a multitude of agencies to help organisations address this critical issue. However, making sense of this alphabet soup of agencies, tools and guidelines can in itself be a significant challenge. From practitioner interviews and a literature review, four broad categories under which the many tools might be grouped for the development of a cybersecurity strategy are identified: frameworks, fundamental controls, risk assessment and capability maturity models.

Building on the findings of the interviews and literature review, recommendations are made for organisations on which specific tools to use within these four categories:

- *frameworks* – adopt the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity.* While small and midsize enterprises (SMEs) do not need to be familiar with the details of this publication, some awareness of the framework's content is recommended.
- *fundamental controls* – implement, as a priority, the six basic Centre for Internet Security (CIS) controls and additional controls for malware defences, firewalls, data backups and secure remote access. These are recommended as the cybersecurity fundamental controls and are applicable to all organisations, from SMEs to multinational enterprises (MNEs).
- *risk assessment* – conduct an enterprise-specific qualitative risk assessment using the CIS Risk Assessment Method (RAM) or possibly the Information Security Forum Information Risk Assessment Methodology 2 (ISF IRAM2), augmented where feasible by the FAIR Institute quantitative approach for organisations that have the necessary analytical capability. Subsequently, develop a plan to implement the risk treatments identified by CIS and ISF, which are NIST aligned. It is recommended that SMEs use only CIS which is more accessible than ISF.
- *capability maturity models (CMMs)* – use the ISF cybersecurity capability maturity model to monitor progress on the organisation's changing security posture over time and cautiously engage in external benchmarking. The use of CMMs and benchmarking is not recommended for SMEs.

While deploying the right tools to mitigate cyber risk is essential, a common theme of the industry practitioners interviewed is that people and process are equally critical. Cybersecurity is not just an IT issue, it is a business issue that must be led by the board and other business leaders. For larger organisations, the importance of making the cybersecurity strategy accessible through the use of real-world cyber threat scenarios and not underestimating the magnitude of the organisation-wide effort required to implement a cybersecurity strategy are also essential.

Although the cybersecurity strategy of any organisation should be based on the nature of the digital assets it holds and controls and an assessment of the risk these assets face, the reality is that smaller enterprises may experience expertise and other resource constraints in conducting this task. Recognising these realities, Section 2.0 presents recommendations on the immediate minimum steps SMEs must take to enhance their cybersecurity posture.

TABLE OF CONTENTS

OVERVIEW

The news of some large-scale data breaches and other cyber disruptions such as those impacting British Airways, Travelex, Facebook and Colonial Pipeline is very widely publicised. However, the extent to which very debilitating cyber incidents happen with very high frequency to enterprises of every size and in every sector is less widely reported.

The first section of this paper explores the background to these circumstances: quantifying the extraordinary growth in electronic data that has occurred this century; the technological factors facilitating this growth; the commercial imperative for enterprises to implement digital transformation; their resulting emergence as data stewards; the vast number of cyber incidents companies are experiencing on a daily basis; the actors behind these incidents and their motivations; and the imperative for enterprises to respond to these developments. While the literature explores many of these matters individually, there appears to be no published work that brings together all of these facets in a succinct format supported by evidence from the literature. Addressing this gap is the objective of the first part of this report. It seeks to help company boards and their executive to understand the scope and scale of the cyber threat and the imperative for them to act.

The need to address this challenge has given rise to an array of frameworks and tools that enterprises might utilise in developing cybersecurity capabilities. Here again, the approach of the literature appears to be to focus on these frameworks and tools disparately, offering little insight into their relative merits and use. Recognising the resource constraints faced by SMEs, Section 2.0 distils the report into a shortlist of immediate, minimum steps that such organisations must take to enhance their cybersecurity posture. Sections 3.0 to 6.0 present the findings of an extensive literature review and research interviews with industry-leading practitioners. Four broad categories of cybersecurity strategy tools available to companies are identified: frameworks, fundamental controls, risk assessment and capability maturity models. The paper groups together the various assets available within these four categories and makes recommendations on which of the tools from each category to use in developing a cybersecurity strategy.

Section 7.0 calls attention to the critical importance placed on people and process by the industry practitioners interviewed, while Section 8.0 discusses some practical considerations in the implementation of a cybersecurity strategy as identified by two leading cybersecurity implementation advisors. Section 9.0 presents a number of emerging trends in the cyber risk and security arena identified by the interviewees, and Section 10.0 concludes with a summary of the paper's findings and recommendations, and the criteria on which these recommendations are based.

The report includes extracts from interviews conducted with experienced cybersecurity, risk and IT practitioners and global cybersecurity implementation advisors. In total 16 interviews were undertaken. 14 of these were with industry practitioners: four Chief Information Security Officers (CISOs), three Information Security Managers (ISMs), five Chief Risk Officers (CROs), a Chief Information Officer (CIO) and an Enterprise Architect (EA). A further joint interview was conducted with the global head and a technical expert of a leading financial services cybersecurity advisory practice. All of the practitioners have group or divisional responsibility with global or large national companies in the financial services sector, are based in Ireland, Germany, Switzerland, the UK and the USA, and represent companies from France, Japan, Switzerland, the UK and the USA. The financial activities the interviewees cover are banking, general insurance, investment management, life insurance and pensions, payments and reinsurance. As financial services are generally heavily regulated and early movers in addressing cyber risk across the globe, it was considered to be a good source of cybersecurity lessons learned. The 14 practitioner interviews explored the experts' use of the artifacts identified in the literature review and the benefits and challenges they faced in their use. For the joint interview with the two global implementation advisors (GIA), the proposed recommendations of the paper were shared with them and their input sought on practical considerations that should be taken into account by organisations when developing a cybersecurity strategy and the implementation of the paper recommendations.

The appendix provides a table of the interviews undertaken, summarises the research method and presents the themes identified from analysis of the interviews.

1.0 THE IMPERATIVE TO ACT

The relentless rise we see in cybercrime today has been facilitated by the exponential growth of electronic data over the last two decades, the diffusion across society of technical innovation and commercial motivation.

1.1 The data explosion

In 2000 analogue media still accounted for 75% of the world's data storage capacity. By 2007 this picture had changed fundamentally with digital assets accounting for almost 95% of the world's storage needs (Hilbert & Lopez, 2011). Since then, the growth in global data has been dramatic, though estimates of this vary considerably. Huadong et al., (2014), projected volumes to grow from 8ZB, $8x10^{21}$ bytes, in 2015 to 40ZB in 2020. A more recent estimate (Reinsel, Ganz & Ryding, 2018) proposes volumes of 33ZB in 2018 increasing to 175ZB by 2025. While the volume estimates do vary, there is consistency in the view that data growth has been exponential in recent years and the outlook is for this trend to continue.

1.2 The diffusion of innovation

This significant growth in data is being facilitated by the diffusion of many technological innovations; the internet, the World Wide Web, broadband, wi-fi, mobile networks, mobile access devices, enhanced data processing and storage capabilities, and cloud computing (Bourgeois, 2019). For example, the number of internet users globally is estimated to have increased from less than 1 per 1000 people in 1990 to almost 460 in 2016, while mobile subscriptions increased from 2 per 1000 in 1990 to more than 1 per head of the world's population in 2017 (Roser & Richie, 2020). The Organisation for Economic Cooperation and Development (OECD) (2013) notes that a major contributor to the growing ubiquity of these technologies is the decreasing costs of internet usage, data processing and storage, and smart access devices. A rapid reduction in cost for comparable performance of technologies such as data storage and processing is charted by Roser and Ritchie (2020). Over the coming five years, much of the data growth forecasted will be from the Internet of Things (IoT). This will be enabled by the diffusion of the fifth generation of mobile technology (5G) and the continued expansion of cloud computing. While 5G will offer improvements in data rate or broadband speeds, the enhancements 5G brings to latency, density and reliability of availability are key considerations for the IoT (NGMN Alliance, 2015).

1.3 Digital transformation and the enterprise as data steward

The last decade has seen a shift from the majority of the world's data being stored by consumers on endpoint devices such as smartphones to the majority of data being stored on enterprise assets (Reinsel et al., 2018). In 2010, consumers were accountable for the creation of approximately 55% of the world's data. In 2017 this consumer portion had dropped to 47% and by 2025 enterprises are expected to account for almost 65% of global data. A key factor in this growth of enterprise data is a desire for organisations to remain competitive and relevant (Hippold, 2018). Businesses are increasingly seeing value extraction from data as a key priority. The International Data Corporation (IDC) & Lisbon Council (2019) estimate that in 2020 almost 750,000 legal entities with employees of 10 or more in the EU and UK will seek to enhance their business through the exploitation of data. If anything, this trend in digitalisation has been accelerated by the Covid-19 pandemic (Baig et al., 2020).

Whether implicitly or explicitly, individuals are facilitating these enterprise data trends through their growing adoption of online services provided by organisations and their increasing dependence on enterprise storage assets. While potentially creating significant new business opportunities for very many companies, this opportunity also brings with it significant new responsibilities. Again, implicitly or explicitly, enterprises are quickly becoming the stewards of the world's data, which they have an increasing obligation to safeguard for business and regulatory reasons. Nowhere is this growing obligation more evident than through Regulation (EU) 2016/679 of the European Parliament and Council, otherwise known as the General Data Protection Regulation (GDPR) (European Council & Parliament, 2016).

1.4 Cyber incidents and data breaches

Cyber incidents and data breaches are an outcome of deliberate or accidental actions by threat actors on information systems, networks and data, or may simply be a consequence of hardware or software failure as noted by the Communications Electronics Security Group (CESG) (2015). While all data breaches are cyber incidents, not all cyber incidents are data breaches, and there is no agreed standard definition of either.

The National Cyber Security Council (NCSC, 2016a) defines a cyber incident as "a breach of a system's security policy in order to affect its integrity or availability and/or the unauthorised access or attempted access to a system or systems; in line with the Computer Misuse Act (1990)". By comparison, NIST (2019) provides a definition of "actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein." As an alternative to referring to cyber incidents, the NIST body of work more commonly uses the term "security incident" which has a definition more comparable to that employed by the NCSC: "An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies".

A concern with the NCSC definition is that it is dependent on the existence of a system security policy, which may or may not be the case for a particular enterprise. While the NIST definition considers the actual or potential violation of security policies also, it is not conditional on organisations having such policies in place.

Regarding breaches, the NCSC (2016b) describes these as "incidents in which data, computer systems or networks are accessed or affected in a non-authorised way". The NIST publication by Cawthra et al., (2019) proposes that data breaches result from failures in data confidentiality while the Information Commissioner's Office (ICO, 2018) also considers it a personal data breach if such data is inappropriately altered or deleted, impacting its integrity or availability.

For the purposes of this paper, apart from references to the ICO where the ICO definition is adopted, the definition of a cyber or security incident used here is that proposed by Verizon (2020): "a security event that compromises the integrity, confidentiality or availability of an information asset". Similarly, the Verizon definition of a data breach is adopted: "an incident that results in the confirmed disclosure – not potential exposure – of data to an unauthorised party".

Concern regarding reputational damage and adverse publicity is a common reason for organisations not to disclose cyber incidents or

data breaches unless this is a legal or regulatory requirement (Fafinski & Minassian, 2009, cited in McGuire & Dowling, 2013; ICO, 2018). Nevertheless, some indication of the enormous extent of incidents can be established from analysis of published sources.

Consider email, for example, which most enterprises still depend on as their primary means of communication and is the key access route into organisations for threat actors (Neely, 2016; Symantec, 2019). Based on the authors' analysis of Clement (2019), Radicati (2019) and Symantec (2019), an estimated 125 billion business emails were sent every day in 2018 of which, annualised, more than 300 million were malicious, containing malware or otherwise perpetrating danger such as through phishing. The European Union Agency for Cybersecurity[1] (ENISA, 2020a) shows that malware was the top cyber threat in 2020 and the threat of phishing attacks continued to increase, with email being the dominant attack vector.

Regarding breaches, Clement (2020) reports that between 2015 and 2019 the annual number of data breaches in the US more than doubled to 1,473 and the number of exposed records over this period was over 1 billion. In the UK, though the number of incidents and the total number of exposed records are not reported, the ICO (n.d.) recorded 1877 personal data breaches resulting from cyber incidents in the 12-month period to the end of September 2019.

1.5 Cyberthreat agents and their motivations

ENISA (2019) identifies seven broad groups of threat agents in order of their reported level of activity:

- Cybercriminals
- Insiders – malicious and negligent
- Nation-states
- Corporations
- Hacktivists
- Cyber terrorists
- Script kiddies

It should be noted that the boundaries between these threat agents are blurred as the characteristics and motivations of the groups are found to be in a constant state of flux.

Cybercriminals are estimated to be responsible for 80% of all cyber incidents. This compares with less than a quarter of incidents experienced by organisations being attributable to malicious and negligent insiders, with employee error accounting for the majority of these insider-driven incidents (ENISA, 2019; OECD, 2017). Based on this distribution, ENISA suggests that companies may be applying a disproportionately high level of security resources to countering the insider threat. However, this view does not appear to take into account the second-order effect whereby malicious actors use email as a primary attack vector and that malicious emails depend on employee carelessness and/or ignorance to be effective. Also, it is proposed that this position does not consider the behaviour prompted by the risk appetite of individuals, which may be very different in the virtual and physical world.

Nation-states, corporations, hacktivists and cyber terrorists are generally focused on very specific targets while script kiddies are considered to be minor actors on the cyber threat stage (ENISA, 2019). These findings are consistent with Verizon (2020) from which the proportion of breaches motivated by financial gain in 2019 is reported to be over 80% and that for espionage at approximately 15%. While the activities of nation-states and their agents are generally focused on a narrow range of targets, the sophisticated tools these perpetrators have developed for their nefarious conduct have become available to other malicious actors, from cybercriminals to script kiddies, thus increasing the threat from these sources.

Criminal online activities previously necessitating specialist capabilities are now being commoditised through the growth of Cybercrime-as-a-Service (CaaS) offering a wide range of tools and resources that significantly reduce the skill requirements of malicious actors (KPMG, 2019; Standard Chartered, 2017). The extent to which CaaS is run as a formal, structured business enterprise is evident from Gross (2021). Symantec (2019) reports a highly active market on the dark web for the data stolen by cybercriminals with, for example, a credit card with full security details selling for $1 to $40, a full ID including bank account details from $30 to $100, and hacked email accounts at $1 to $15 per

1 The name of the European Network and Information Security Agency (ENISA), created in 2004, was changed in 2019 to the European Union Agency for Cybersecurity while retaining the original ENISA acronym.

2,500. Trojan toolkits with support for banking and a distributed denial of service (DDoS) attack incapacitating a victim's website for more than 24 hours are examples of CaaS offerings available for prices ranging from $10 to $1,500 and $10 to $1,000 respectively.

1.6 The implications for enterprises

Major data breaches such as that suffered by Experian, Travelex, Facebook and Microsoft attract press headlines, but SonicWall (2021) and Symantec (2019) show that companies of all sizes, including the very smallest, and across all industry sectors are subject to constant cyber threat and attack. The UK Department for Digital, Culture, Media & Sport (DCMS, 2020) discusses the difficulty in determining the cost of such activities on organisations and this difficulty is reflected in a wide range of reported numbers for breach costs. The Federation of Small Business (FSB, 2019) reports the UK small business community suffers almost 10,000 attacks daily at an annual cost of £4.5b. Accenture (2019) suggests an average cost of $13m for all companies globally incurring a data breach. By comparison, IBM (2019) reports an average cost of almost $3m for a data breach of an enterprise with less than 500 employees compared to $5m for companies with over 25,000 employees. These lower costs proposed by IBM compared to Accenture can be explained by the former's exclusion of the distorting cost of "mega breaches" and only examining breaches compromising record numbers ranging from 2,000 to 100,000. Another analysis of 2,081 actual cyber insurance claims between 2014 and 2018, of which 787 related to data privacy breaches, reported average breach claim costs of $178k and $5.6m for SMEs and large companies respectively (Netdiligence, 2019). Though significant, these actual claims figures do not reflect the increased costs associated with potential fines of €20m or 4% of global revenue that can be imposed under the GDPR which came into force in 2018. Also, the definition of an undertaking used in the GDPR to determine the scope of a data breach fine is very far-reaching. It allows a fine to be based on the global revenues of any company with economic activity in Europe, regardless of where the company is based in the world. Also, the revenues of any parties exerting significant influence, such as joint venture partners, can be included in a fine assessment (Mayer Brown, 2018).

Although estimates and definitions of many metrics relating to cybersecurity vary widely, what is clear is that enterprises have a rapidly growing dependency on data for the success of their businesses, while cyber threats are becoming ever-more pervasive and the consequences of these threats materialising are becoming increasingly onerous. In 2017 the NCSC & NCA (2017) asserted that no organisation is safe from cyber threat and PwC (2017) posited that an attack is inevitable. This reality is even more pronounced today with the rise of ransomware (Warrell, 2021). Yet, despite the pernicious and growing threat, there is a concern that companies and their boards are not doing what needs to be done to address it. In her first public address (NCSC, 2021a) the new CEO of the UK NCSC observed:

> Cybersecurity is still not taken as seriously as it should be…the pace of change is no excuse – in boardrooms, digital literacy is as non-negotiable as financial or legal literacy.

There are steps that organisations can and must take to minimise the impact of cyberattacks. As Crotty (2019) notes regarding cybersecurity, company directors are legally bound to take such steps as are reasonable under the UK Companies Act (2006). CIS (2018) points to a similar requirement for reasonableness by the US courts and also the duty of care enterprises have in their conduct of cybersecurity.

2.0 FOR SMES – IMMEDIATE, MINIMUM STEPS

Although the findings of this report are based largely on the insights of leading cybersecurity and risk practitioners from global companies and/or domestic household names, a number of the recommendations are imperative for organisations of all sizes, from SME to global operators. While the rationale for these recommendations is explored in detail in the subsequent sections of the report, recognising the reality of resource constraints that SMEs may face, a summary of the recommendations on the immediate minimum steps SMEs must take to enhance their cybersecurity posture is presented here.

The Framework for Improving Critical Infrastructure Cybersecurity, published by the US Government's National Institute of Standards and Technology (NIST) is emerging as a de facto cybersecurity reference document with its framework and language being widely adopted by practitioners, advisors, regulators and other agencies of nations across the world (NIST, 2018). While detailed knowledge of this publication is not required by SMEs, some awareness of the NIST framework's five functions – identify, protect, detect, respond, recover – is recommended as these terms have become ubiquitous in use across the cybersecurity industry including supernational agencies such as the Australia Cyber Security Centre (ACSC), the European Union Agency for Cyber Security (ENISA), and the UK's National Cyber Security Centre (NCSC).

The Centre for Internet Security (CIS) has identified six basic controls for deployment by organisations (CIS, 2019). Based on a review of essential controls proposed by the ACSC, ENISA and the NCSC, the recommendation in this report is that SMEs should deploy the six basic controls proposed by CIS and the additional controls for malware defences, firewalls, data backups and secure remote access as advised by these national and supernational agencies. More detail on these controls is provided in Section 4.0.

While implementing the ten fundamental cybersecurity controls recommended here is essential for every organisation, these technical measures are not sufficient. It is also critical that all employees are made aware of the risk posed to the organisation and themselves by poor online security practices. The UK NCSC *Small Business Guide: Cybersecurity*, first published in 2018 and reviewed in 2020, gives guidance on the steps that organisations can take to facilitate this (NCSC, 2018a).

The NIST, CIS and NCSC materials cited in this section are freely available online through the links provided with the citations.

3.0 DEVELOPING A CYBERSECURITY STRATEGY

The cybersecurity countermeasures needed by companies incorporate technology, people and processes (NCSC & NCA, 2017). The literature describes many different frameworks and tools that organisations might use in addressing this challenge. However, the discussion in the literature explores the use of these tools on a discrete basis rather than how they might be used together by an organisation to address their cybersecurity needs. This paper proposes that the multitude of tools should be considered within four broad areas:

- frameworks
- fundamental controls
- risk assessment
- capability maturity models

The next section of this paper explores a range of the tools within each of these categories. It examines how the different categories might be brought together by an organisation in a unitary approach to develop a cybersecurity strategy incorporating reasonableness and duty of care considerations.

3.1 Cybersecurity frameworks

The NIST cybersecurity framework was first published in 2014 in response to US Executive Order 13636 intended to improve the US's critical infrastructure risk (Obama, 2013). In 2015, Shackleford, et al., (2015), proposed that the NIST framework had already influenced national thinking on cybersecurity practices well beyond the US, but that time would be required to determine the extent to which this framework might prove to be norm building. The NIST approach aims to achieve desired cybersecurity outcomes through activities utilising existing and regularly updated best practice, tools and standards. The work is based on a core framework comprised of four elements: Functions, Categories, Subcategories and Informative References. (See Figure 1). The work proposes that five functions form the foundation of cybersecurity activity; Identify, Protect, Detect, Respond and Recover. Each of these functions is mapped onto Categories and Subcategories showing recommended cybersecurity activities in increasing detail, and the Informative References section is a catalogue of tools and standards that might be used to facilitate these activities to achieve desired cybersecurity outcomes.

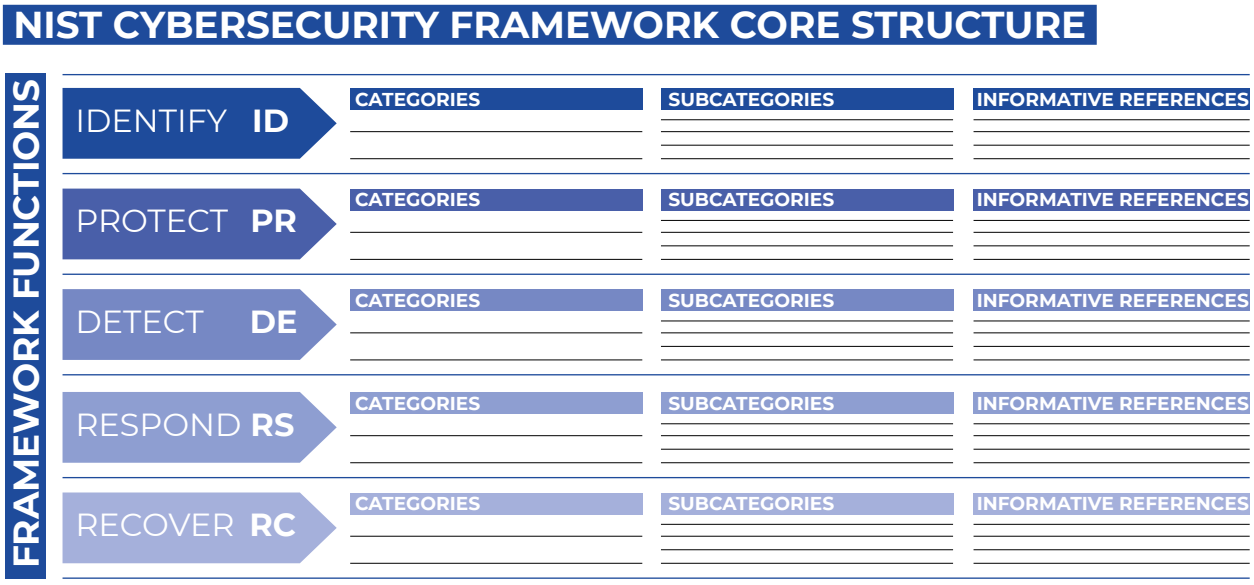

Figure 1: NIST cybersecurity framework core structure
Source: NIST Framework for Improving Critical Infrastructure Cybersecurity (2018).

Despite differences in national approaches, the influence of NIST is acknowledged in the works of other nations and a degree of commonality of overall approach and wording is evident, particularly in the adoption of NIST's five framework functions. (See Table 1). In this respect, NIST (2018) is unique compared to other frameworks.

EXAMPLES OF INTERNATIONAL ADOPTION OF THE NIST CYBERSECURITY FRAMEWORK FUNCTION TERMINOLOGY

NIST cybersecurity framework functions [1]	Australia ACSC cybersecurity principles[2]	EU ENISA 'Get prepared for the next cyber crisis'[3]	EU NIS Directive[4]	Italy CINI Framework Naz. per la Cybersec. e la Data Protection[5]	UK GFS Minimum Cybersecurity Standard[6]	UK NCSC Incident Management[7]	UK NCSC CAF[8] Guide
Identify	Govern: **identify** & manage	**Identify**	**Identify**	**Identify**	**Identify**	**Identify**	Manage: **identification**
Protect	**Protect**	**Protect**	**Prevent**	**Protect**	**Protect**	**Protect**	**Protecting**
Detect	**Detect**	**Detect**	**Detect**	**Detect**	**Detect**	**Detect**	**Detecting**
Respond	**Respond:** responding & **recovering**	**Respond**	**Handle**	**Respond**	**Respond**	**Respond**	Minimising: **response** & **recovery**
Recover		**Recover**	**Mitigate**	**Recover**	**Recover**	**Recover**	

Table 1: Examples of international adoption of the NIST cybersecurity framework function terminology (Source: Authors' own analysis of NIST, 2018[1]; ACSC, 2020a[2]; ENISA, 2018[3]; European Commission, 2016[4]; CINI, 2019[5]; GFS, 2018[6]; NCSC, 2019a[7]; NCSC, 2019b[8])

3.2 Cybersecurity frameworks – a practitioner perspective

The interviews with cybersecurity practitioners indicated that while there are limitations with all of the frameworks reviewed, NIST is becoming increasingly ubiquitous. For example, the CISO of a leading general insurance firm valued its global recognition and constant improvement, which is important when threats are constantly evolving. Similarly, the group CISO of a leading reinsurance firm also noted the strength of NIST in its acceptance by regulators:

> *SE CISO:* We are aligned with NIST. It is a really good framework with lots of US money going into it. It is constantly being improved and is globally recognised.

> *RT EA:* NIST is free, ubiquitous, uses a common industry language and is much more accessible than the ISO suite.

> *OL CISO:* If I talk with regulators and clients, they view NIST as best practice. It also offers supporting materials.

> *MS ISM:* From a controls perspective, the ISO suite does not provide the same level of detail as other guidelines.

> *LM CISO:* The value of ISO certification is highly questionable. Certification can be achieved even if the scope of the certification is inadequate. It is like saying my house is certified as secure even though I don't have a front door because this was not in the scope of my certification.

The EA of a life insurance and pensions company feels NIST provides a consistent and shared language for all users and is much more accessible than ISO 27000. Others note the scope of ISO 27000 is limited with a focus on policy and minimal guidance on controls, and the merit of ISO certification is also questioned. Amongst those interviewed, there is a very clear preference for the use of the NIST Cybersecurity Framework over the ISO 27000 suite.

3.3 Cybersecurity frameworks – recommendation

In addition to the growing adoption of NIST (2018) across the globe, including widespread acceptance by regulators, NIST is considered to work well as a framework for organisations in bringing some order to the "alphabet soup" of cybersecurity tools. There is also evidence from cybersecurity practitioners that the solutions offered to organisations by cybersecurity industry vendors are beginning to coalesce around needs identified through the NIST framework. For these reasons the approach recommended here is for organisations to use the NIST framework for development of a cybersecurity strategy and cross-reference this against their national framework, if relevant, to ensure adherence to any unique domestic requirements such as, for example, those specified in Germany's *IT-GrundschutzKompendium* (BSI, 2020).

4.0 CYBERSECURITY FUNDAMENTAL CONTROLS

The fundamental objective of cybersecurity is to implement controls that seek to prevent threats from exploiting vulnerabilities in information systems resulting in harm that compromises the confidentiality, integrity and availability of information assets (ISO, 2013a; ISO, 2013b; Pfleeger et al., 2015). Recognising the multifaceted nature of cyber threats and vulnerabilities, these ISO publications (2013a & 2013b) and others such as CIS (2019) require the implementation of a range of complementary and compensating controls to provide cybersecurity defence in depth. NIST (2020a) also presents a suite of controls and both it and other artifacts such as ISO 27001 (ISO, 2013a) are included as Informative References in the NIST cybersecurity framework to help facilitate cybersecurity implementation (See Figure 1).

ISO 27000 (2013a) offers a suite of 114 possible controls for organisations to deploy but provides no guidance on which controls to prioritise, and specifically mentions that no prioritisation is inferred by the order in which the controls are presented. The same is true of NIST (2020a) which identifies 320 possible controls though the related publication, NIST (2020b), does seek to facilitate the selection of controls by listing a range of three baseline control configurations commensurate with an organisation's perceived security needs.

However, even then, 180 controls are proposed for the lowest-ranked of these configurations.

Of the various suites of controls cited in the NIST Informative References, CIS (2019) offers the most concise guidance on control implementation sequencing and prioritisation. CIS (2019) lists 20 controls across three categories; Basic, Foundational and Organisational, with these categories having six, ten and four controls respectively. See Table 2. The 20 controls in turn incorporate a total of 171 sub-controls split 47, 88 and 36 across the three categories. Within these categories, CIS further differentiates control implementation requirements between three groups of organisation types based on size and level of technical sophistication. Consequently, as shown in Table 2, a small to medium-sized organisation with limited technical capabilities is required to implement 11 Basic sub-controls, while a large technically sophisticated firm is required to implement the full suite of 47 Basic sub-controls.

CIS (2019) proposes that the Basic sub-controls it has identified for its three organisation types are a prioritised set of hygiene controls that must be implemented by every organisation and seek to balance the need for risk mitigation with an organisation's resources and capabilities.

CIS CONTROLS AND SUB-CONTROLS BY CATEGORY AND IMPLEMENTATION GROUP

Control categories	Basic	Foundational	Organisational
Controls per category	6	10	4
Sub-controls per category	47	88	36
Implementation Groups	Sub-controls per implementation group		
Group 1 : Limited resources	11	22	11
Group 2 : Moderate resources	38	69	33
Group 3 : Significant resources	47	88	36

Table 2: CIS controls and sub-controls by category and implementation group

Source: Authors' own analysis of CIS (2019)

The publication further asserts that the CIS control selection and prioritisation is based on the experience and recommendations of an ecosystem of experts and organisations that have deployed the CIS controls, though it should be noted that no supporting evidence for this view is provided. Nevertheless, some evidence of support for this position regarding the proposed controls can be found elsewhere. See Table 3.

MAPPING OF GOVERNMENT AGENCY CYBERSECURITY FUNDAMENTAL CONTROLS TO CIS CONTROLS

CIS [1]	Cyber Essentials [2]	Essential Eight [3]	Top ten cyber hygiene tips for SMEs [4]
Basic control 1: Inventory and control of hardware assets	***Scope*** of devices and software to be protected to be determined. Malware protection applied – anti-malware software, ***application allow listing*** or application sandboxing – to ***restrict execution of*** known malware and ***untrusted software***.		***Risk assessment. Identify and prioritise the main assets*** and threats.
Basic control 2: Inventory and control of software assets		***Application control*** --- ***User application hardening***	
Basic control 3: Continuous vulnerability management	***Patch management***	***Patch applications*** --- ***Patch operating systems***	***Updates.*** Keep everything up to date including security updates.
Basic control 4: Controlled use of administrative privileges	***User access control***	***Restrict administrative privileges***	***Access management***
Basic control 5: Secure configuration for hardware and software on all devices	***Secure configuration***	***Configure Microsoft Office macro settings*** to block macros from the internet.	
Basic control 6: Maintenance, monitoring and analysis of audit logs.			
Foundational control 8: Malware defences	***Malware protection applied***		***Endpoint protection***
Foundational control 10: Data recovery capabilities		***Daily backups***	***Backups***
Foundational control 11: Secure configuration for network devices, such as firewalls, routers and switches	***Firewalls must be actively managed***		
Foundational control 12: Boundary Defence		***Multi-factor authentication***	***Secure remote access***
Organisational Control 17: Implement a security awareness and training programme			***Awareness***
Organisational control 19: Incident response and management			***Incident management plan***
N/A			***Management buy-in***
N/A			***Cybersecurity policy***

Table 3: Mapping of government agency cybersecurity fundamental controls to CIS controls

Source: Authors' own analysis of CIS (2019)[1], ACSC (2020b)[3], ENISA (2020)[4] and NCSC (2021b)[2]

The Australian Cyber Security Centre (ACSC, 2020b) and NCSC (2021b) are, respectively, Australian and UK government agency publications identifying minimum cybersecurity controls required for organisations to do business with Australian and UK government entities, and ENISA (2020) is an EU document offering cybersecurity hygiene recommendations for small and midsize enterprises. While none of these three reference documents map precisely to one another or to CIS (2019), it is clear from Table 3 that there is some degree of alignment in the recommended controls across the four artifacts, particularly the six basic controls proposed by CIS. The German government agency, Bundesamt für Sicherheit in der Informationstechnik (BSI), also prescribes a list of controls categorised as Basic, Standard and Increased Protection Needs, (BSI, 2020). However, as even the BSI basic controls are very extensive and no implementation prioritisation is recommended, these controls are not comparable with the requirements identified in Table 3.

Management of audit logs is the only basic control that CIS alone recommends. Apart from ENISA (2020), which includes four organisational controls, all of the basic and essential controls identified by the four agencies are IT system operation and access controls with limited dependency on employees for compliance. While malware defences, firewalls, data backups and secure remote access including multifactor authentication are not proposed as basic controls by CIS, they are requirements of one or more of the other agencies. Though not included in the CIS basic controls it should be noted that these four controls can play an important part in providing defence in-depth and countering the threat of ransomware, which is becoming increasingly prevalent (Warrell, 2021).

4.1 Cybersecurity fundamental controls – a practitioner perspective

The importance of prioritisation of controls is recognised by practitioners but so is the need to move quickly beyond implementing hygiene factors to the conduct of penetration testing or "pen-testing". Pen-testing is conducted by ethical hackers engaged by an organisation to proactively identify vulnerabilities in the organisation's networks by replicating the actions of unethical hackers. The effectiveness of continuous pen-testing compared to other possible approaches such as intermittent control audits is emphasised.

RT EA: NIST has a very comprehensive set of controls sitting behind the cybersecurity framework. The value of CIS is that it brings prioritisation that doesn't exist in the NIST or ISO frameworks.

CG CRO: An external audit of a control shows if a control is in place or not. Similarly, periodic pen-testing shows an issue in the moment but doesn't show how effective controls are over time. Such audits and periodic testing are not nearly as valuable as having a team conducting continuous pen-tests, over and over again.

DT ISM: Getting to green on hygiene factors is not enough. These are only the very basic requirements. This is where companies start but then take unwarranted comfort when the basic controls are green. Pen-testing is not considered a hygiene factor but it is critical. Getting the board and executive to understand we must move beyond hygiene factors is a struggle.

A constant challenge for practitioners is ensuring that companies and their boards understand that the implementation of fundamental cybersecurity controls is merely the start of the process in developing a cybersecurity capability. This observation echoes the recent concern of the UK NCSC CEO regarding the approach of boards to the issue of cyber risk and their need for far greater understanding of the subject matter (NCSC, 2021a).

4.2 Cybersecurity fundamental controls – recommendation

Although practitioners cite the critical importance of pen-testing, and some suggest it should be considered a hygiene factor, it must be recognised that the purpose of pen-testing is to determine the effectiveness of established cybersecurity controls. While pen-testing can be of critical value in enhancing an organisation's cybersecurity posture, it should only be undertaken when other basic controls have already been implemented.

It is recommended here that the six basic CIS controls and malware defences, firewalls, data backups and secure remote access including multifactor authentication as proposed by other agencies, and described in Section 2.2, should be considered cybersecurity fundamental controls. While the full suite of controls an organisation deploys should be determined by an organisation-specific risk assessment as discussed in the next section, the cybersecurity fundamental controls identified here should be adopted by all organisations as a priority and subsequently refined based on the findings of a risk assessment.

5.0 CYBER RISK ASSESSMENT

While it is essential that organisations implement the controls identified as cybersecurity fundamentals, this step can only be viewed as addressing basic hygiene factors. The purpose of these controls is to help mitigate the most common cyber risks experienced by organisations on a generic basis (CIS, 2019; NCSC, n.d.). Further to the implementation of these fundamental controls, a bespoke risk assessment should be conducted reflecting the enterprise's specific circumstances. This process needs to consider the type and level of risk the organisation can accept, taking into consideration the nature of its information assets, the threats and vulnerabilities these assets are exposed to, the likelihood of these threats materialising, and the resulting impact on the assets and stakeholders. This is a standard approach to defining risk criteria and risk assessment and is comprised of risk identification, analysis and evaluation (ISO, 2018; Lam, 2017), Figure 2. From this risk assessment a company-specific plan can be established that considers the four options for risk management – avoid, reduce, transfer or retain (NCSC, 2018b).

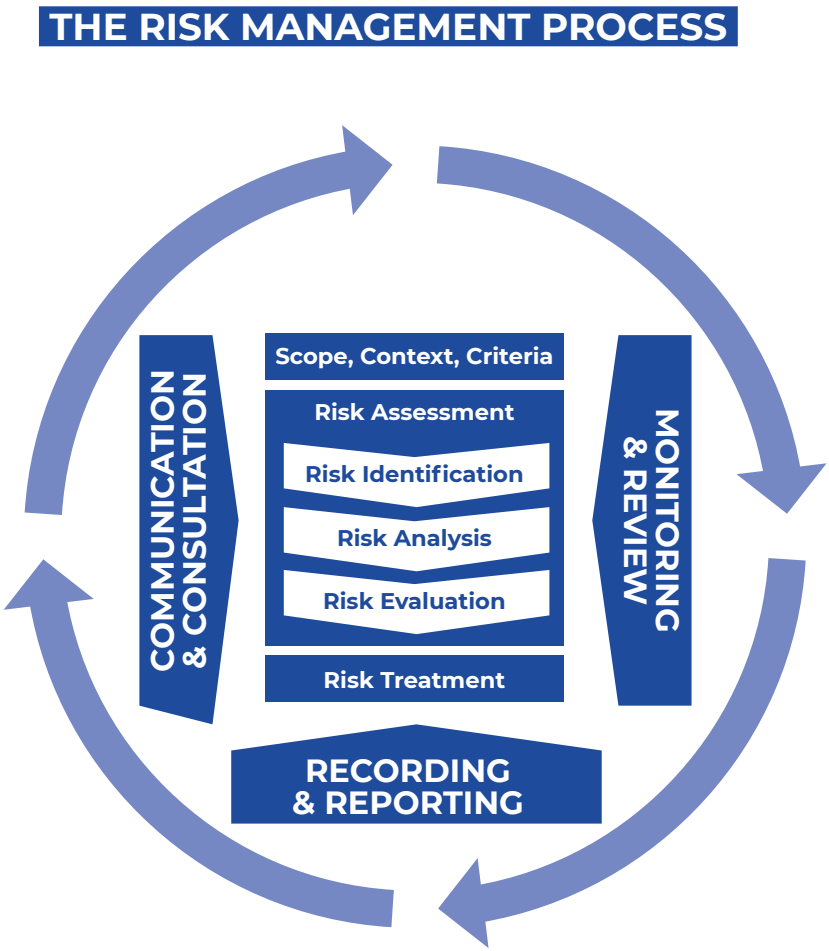

Figure 2: The risk management process
Source: BS ISO 31000:2018: Risk management. Guidelines (2018).

There are many published risk management and assessment models and tools that might be utilised by an organisation in the conduct of a cyber risk assessment. An early study by ENISA (2006) provides details of 25 such artifacts, including a comparison table of 13 models. Heidt et al., (2014) reviewed eight risk assessment and analysis approaches selected on a number of criteria, including evidence that they have been used in practice and are currently maintained by their publishers. All but one of these eight frameworks is based on ISO 31000 which the authors observed was becoming the de facto risk management standard on which risk assessment processes are based.

Like the ISO 31000 framework, many of the assessment and analysis artifacts presented by ENISA (2006) and Heidt et al. (2014) originated to address broader enterprise or IT risk management needs. However, a number of methods and tools, including some more recent materials, focus specifically on information security while using an approach that is consistent with ISO 31000. These works include CIS RAM, FAIR, ISF IRAM2, ISO 27005[2] , ISMS[3] , MAGERIT[4] , NIST SP 800-30, Octave Allegro and OWASP[5] (CIS, 2018; Open, 2010; Freund & Jones, 2015; ISF, 2017; BSI, 2017; Amutio et al., 2014; NIST, 2012; Caralli et al., 2007; Williams, n.d.). ISACA's COBIT2019 is another commonly referenced approach though this is not based on ISO 31000 (ISACA, 2018). A key differentiator between these ISO 31000 based tools is the use and consideration of a quantitative verses qualitative approach for risk analysis.

From the list, FAIR alone adopts purely quantitative techniques, employing Bayesian probability methods and the use of Monte Carlo Simulation (MCS) to determine risk impact and probability. MAGERIT offers qualitative and quantitative approaches which CIS RAM also refers to, while the remaining works are purely qualitative, relying on ordinal scales for ranking risk impact and likelihood.

With only limited data available, Bayesian methods facilitate the use of subjective judgement to select probability distributions for different cyber risk events and a combined distribution for all these events can be determined using MCS (IBM, 2020). As MCS requires significant computer processing power its use in recent years has been fuelled by many of the same technology enhancements that have driven the rise of cyber risk as discussed in Section 1. These quantitative tools have already entered common usage in disciplines such as project management, finance, engineering and software development over the past decade (Pergler & Rasmussen, 2014; Thelin, 2018; Yano et al., 2012, Kroese et al., 2014) but the deployment of such tools in managing cybersecurity risk is still nascent. NIST (2012) proposes that the qualitative methods available for risk management are easier to understand, implement and explain as required for all those involved in the cybersecurity process, from cybersecurity professionals to the board. However, this does not make qualitative methods preferable. Hubbard and Evans (2010) propose that this approach, incorporating ordinal scales and/or a two-dimensional probability and impact risk matrix, has four fundamental flaws. First, they contend that such methods typically fail to take into account the bias of users in their subjective assessment of risk. Second, ordinal scales commonly use verbal labels which are inconsistently interpreted by different users and indeed by the same user over time. Third, where numerical labels are used in ordinal scales the values of these labels are frequently combined arithmetically even though such numeric operations are not mathematically logical as the distance between the points on an ordinal scale is indeterminate. The fourth concern raised is that such qualitative methods rarely account for risk correlations that could significantly impact the outcome of a risk assessment. Cox (2008) raises a further issue he calls "range compression" that can result in risks of very different magnitude being assigned exactly the same rating in a risk matrix. Hubbard & Seiersen (2016) explain that range compression is a consequence of partitioning the continuous values to probability and impact into the discrete ordinal value labels of a risk matrix. Advocates of quantitative methods contend that any use of such qualitative approaches is unsound. They also assert that the apparent precision of the output of qualitative methods can lead to a false sense of confidence in the rigour of the analysis and results on which cyber risk mitigation plans will be based (Krisper,

2 A revised version of BS ISO 27005:2011 is under development. To fill the interim gap, BS 7799-3:2017 has been published to align with the requirements of BS EN ISO/IEC 27001:2017.

3 Information Security Management System

4 Methodology for Information Systems Risk Analysis and Management

5 Open Web Application Security Project

2021; Hubbard & Seiersen, 2016; and Freund & Jones, 2015).

Like NIST (2012), NCSC (2018a) emphasises the importance of ensuring clear communication and understanding between those who analyse risk and those who make decisions based on this analysis. But, unlike NIST which advocates a quantitative approach for this reason, NCSC refers to the benefits of considering both qualitative and quantitative methods.

Although the mathematical properties of probability theory permit analyses that are not possible using ordinal numbers and risk matrices, there are other significant constraints on the use of quantitative methods that need to be taken into consideration. The mathematical rigour on which quantitative analysis is based can lead to a false sense of confidence in the results, which is the same valid concern raised regarding qualitative methods that subject ordinal scales to mathematical operations. The reality is that the input for both methods is largely based on the opinion of subject matter experts augmented by whatever data may be available. Of necessity, this expert opinion, which may be subject to bias resulting in over or under confidence, is reflected in the output of the risk analysis regardless of whether a qualitative or quantitative approach is used (Dhami et al., 2015; Sharot, 2011). Also, the need to have an understanding of the probability theory underlying quantitative methods may prove challenging for many organisations. If quantitative methods are to be used it is essential that these methods are transparent to those whose expert judgement is needed.

Considered in the context of the obligations that organisations and their boards have to their stakeholders, (Crotty 2019; CIS 2018), and the legal and regulatory implications of this including the potential for significant fines, it is clear that every institution must decide which cyber risk analysis approach it wishes to use and why, and also ensure they understand the relative merits and constraints of the approach they choose. Furthermore, given the tightening legal and regulatory regime, those typically larger and/or more specialist organisations that have the analytical expertise required to support quantitative risk analysis methods, but choose not to use these capabilities in addressing their cyber risk analysis, may find themselves under more intense scrutiny in the event of a cyber incident that causes stakeholder harm.

5.1 Cyber risk assessment – a practitioner perspective

Amongst practitioners, opinion varies on the relative merits of the use of qualitative and quantitative analysis in risk assessment with most seeing strengths and weaknesses in both approaches.

The CRO of a major UK asset management firm expresses concern at the “false science” of risk matrices but also cautions on the limitations of quantitative approaches, while the CISO of a global reinsure notes the importance of using both methods.

> *TOK CRO:* Some people love to have a 3x3 or 5x5 matrix for risk assessment, but this can result in a false science. It makes me feel quite nervous. This approach can result in a sea of green but all around there are dozens of exceptions to policy which, when added up, are far from the sea of green.

> *TOK CRO:* Going down a quant route is fine if you have a sense of what is the worst that could happen. But because cyber threats change so fast I don’t see how anyone can look forward and reasonably project possible outcomes.

> *OL CISO:* While we use a quantitative approach to determine our capital requirements, we also see a use for qualitative assessment based on expert judgement.

The CISO of a global payments firm notes that they are investing in developing quantitative capabilities but there are cases where quantitative methods remain more appropriate. And the CRO of a major insurer also cautions on blindly accepting the output of a quantitative model.

> *GH CISO:* We do an annual risk assessment of the entire programme that uses both quantitative and qualitative techniques. Where we can used data driven approaches we do. We have invested heavily in a capability that allows us to do this but there are times when it is still tradecraft.

BN CRO: The quant approach to operational risk ends up forcing one down a route where the numbers tell you what you must do or how you must rate things, but when you reflect on the outcome you feel you quite often have the wrong answer. And you also get a lot of people doing a lot of counting but not a lot of thinking.

The challenge of presenting the findings of quantitative analysis to those that are not subject matter experts is also recognised by the CISO of a major general insurer.

SE CISO: We try to use the FAIR model as much as we can instead of a risk matrix. We try to think about distributions and probabilities, but we do not take this level of detail to the board. We have to present our statistical analysis using a risk matrix and RAG ratings.

The ISM of a global insurance firm notes that the availability of sufficient data for use in quantitative methods is currently seen by some to be a limitation, but this will change over the coming years as a body of cyber risk data is accumulated. This ISM sees the use of quantitative methods in cyber risk management as inevitable.

MS ISM: Data is a constraint for the use of quants now, but this will change over time. Sooner or later quants will have to be used for cyber risk capital allocation. How accurate this will be no one knows but this is the same for many risks.

And finally, the divisional head of a global bank offers a caution for firms on the implications of not using quantitative methods to guide the strengthening of their cybersecurity posture if they have the capabilities.

CN CRO: An organisation with the capability to conduct quantitative cyber risk analysis but not doing so may face additional exposure should a cyber incident occur. Was it reasonable for them not to take this step in seeking to protect their stakeholders?

As more data is gathered on cyber risk events the use of quantitative analysis in risk assessment is expected to become increasingly pervasive but, based on current views, it is likely that this emerging capability will augment rather than displace the widely used qualitative approach.

However, regardless of what method of risk analysis is employed – qualitative, quantitative or some combination of both – the output must never be blindly accepted. It is imperative to ask if the results seem reasonable and make sense in the real world (Thompson & Smith, 2019).

5.2 Cyber risk assessment – recommendation

The approach to cyber risk analysis advocated in this paper calls on the experience of risk analysis in other more established disciplines in which both qualitative and quantitative methods are considered to have merit. In project management, Safran (2021) contends that neither approach has supremacy; that quantitative risk analysis should follow a broader more general qualitative assessment. Similarly, Thelin (2018) and Pergler and Rasmussen (2014) present cases for the use of MCS and Bayesian methods to augment, not replace, more traditional methods of analysis. Triangulation of this nature can help provide a better understanding of the uncertain nature of cyber risk (Salkind, 2010). This recommendation is consistent with the view of cyber risk practitioners.

Although many of the published qualitative assessment tools are very similar in their approach, the segmentation by organisation type, inclusion of a NIST-aligned suite of controls and provision of some insight into quantitative methods makes CIS RAM the preferred qualitative framework. An alternative for consideration is ISF IRAM2. This also offers a suite of controls and is unique in offering a benchmarking capability which, despite limitations discussed in the next chapter, does have some benefit.

Organisations with the capability to utilise quantitative analysis methods in cyber risk assessment should do so as it will offer an alternative perspective for consideration and may become an important factor in the assessment of companies by regulators in the event of a breach. Organisations conducting quantitative analysis should refer to FAIR and also Hubbard & Seiersen (2016).

6.0 CYBERSECURITY CAPABILITY MATURITY MODELS

Capability Maturity Models (CMMs) have their origin in a process-maturity framework developed by the Software Engineering Institute in the 1980s (Humphrey et al., 1987). Devised to improve the quality of software produced by vendors for the US government, CMMs are now widely applied to processes beyond software development including assessing the maturity of the implementation of cybersecurity controls. This evolution is reflected in the international standard defining the measurement framework for process capability (BSI, 2019). Consistent with earlier versions, the most recent update of this standard refers to information technology in its title, but the body of the document now asserts its applicability to processes in general without specific reference to information technology and software development.

While there are many CMM design variations, a fundamental characteristic of them all is that they determine levels of performance maturity for an organisation process based on indicators showing the effectiveness of the process in achieving its objectives. (BSI, 2019; Rea-Guaman et al., 2017a). Rea-Guaman et al., (2017b) identify nine CMMs used to measure cybersecurity control processes. While process steps and indicators of effectiveness are organisation specific, BSI (2019) identifies six performance maturity levels that must be used for a CMM to conform to the ISO standards. See Table 4.

CAPABILITY MATURITY MODEL PROCESS CAPABILITY LEVELS

Maturity level	Capability	Outcome
Level 0	Incomplete process	The process is incomplete or fails to achieve its process purpose.
Level 1	Performed process	The implemented process achieves its process purpose.
Level 2	Managed process	The Performed process is now implemented in a managed fashion – planned, monitored and adjusted – and the process documentation is appropriately established, controlled and maintained.
Level 3	Established process	The Managed process is now implemented using a defined process which is assured and continuously improved.
Level 4	Predictable process	The established process now operates predictively to achieve its process outcomes. Quantitative management needs are identified, measurement data are collected and analysed to identify assignable causes of variation. Corrective action is taken to address such variation.
Level 5	Innovating process	The process innovation attribute is a measure of the extent to which changes to the definition, management and performance of the process are identified and effectively implemented from identified approaches for process innovation using internal resources and/or external ideas according to defined process innovation objectives.

Table 4: ISO capability maturity model process capability levels
Source: BSI (2019)

BSI (2015) identifies process performance improvement, assessment of process-related risk and benchmarking across organisations as objectives for the use of CMMs. However, considerable caution must be taken when using a CMM for any or all of these purposes even if it conforms to the ISO standards, as the validity of CMMs is subject to the same challenges as qualitative risk assessment methods proposed by Hubbard and Evans (2010) discussed in Section 4.0. Apart from depending on the subjective view of those conducting a process maturity assessment, CMMs utilize an ordinal ranking of process maturity levels. Furthermore, the ISO standards, (BSI 2019), permit the addition, subtraction and averaging of these ordinals which have no mathematical validity whatsoever. In such cases, the maturity ranking of a typical control is determined by mean averaging the ordinal ranking of its sub-controls but this averaging, which in itself is mathematically invalid, can mask the presence of weak sub-controls and provide a more optimistic assessment than the reality warrants.

These concerns, and ignorance regarding the context and motivation of an organisation undertaking a CMM assessment, mean that the use of published CMM results for benchmarking between groups of organisations must be considered a questionable practice. This view regarding the use of CMMs for cybersecurity benchmarking purposes is supported by the decision of the NCSC to withdraw its Information Assurance Maturity Model (IAMM) in 2018, citing its applicability for benchmarking as a concern (NCSC, 2018c).

However, if these limitations are understood and taken into consideration, CMMs do have merit in helping organisations to track the evolution of their own cybersecurity capabilities over time and help prioritise the cybersecurity effort by identifying potential areas of weakness that warrant further investigation.

A factor that may have a significant bearing on the future deployment of capability maturity models in assessing the cybersecurity posture of organisations is the introduction by the US Department of Defence (USDoD) of a supplier cybersecurity certification regime based on a cybersecurity maturity model (USDoD, 2020a). This comprehensive model seeks to combine the best cybersecurity practices and controls identified from multiple agencies across the globe. It categorises this array of practices and controls into five practice levels from Level 1, Basic Cyber Hygiene with 17 cybersecurity control practices and progresses to Level 5, Advanced/ Progressive with 171 practices. A process maturity assessment is then overlaid on these practices starting at Level 1, Performed progressing to Level 5, Optimizing. While similar in approach to the work presented in Section 3.0, the basic requirements stipulated for suppliers to the USDoD are more onerous than the fundamental controls recommended in this paper. Apart from the 11 controls recommended in Section 3.0, any subsequent control requirements are determined from a bespoke risk-based approach as described in Section 4.0. By comparison, the USDoD is again more onerous with all of its controls being mandatory unless clearly and demonstrably inapplicable and this inapplicability is validated by a USDoD approved external assessor.

While incorporating a framework of advancing levels of process maturity for cybersecurity practices similar to other CMMs, the USDoD approach also has a number of fundamental and important differences. The USDoD Cybersecurity Maturity Model Certification (CMMC) does not entail the application of mathematical operations on ordinal numbers as used by many other maturity models. To achieve certification at a particular cybersecurity practice level an organisation must be able to demonstrate that it effectively deploys all the controls required for that level unless a given control clearly does not apply to a particular organisation. Certification can only be granted by USDoD approved certifying bodies which are required to evidence the implementation of the required controls. Furthermore, unlike some cybersecurity frameworks (CIS 2019) which differentiate between the controls required based on organisation size and sophistication, the USDoD expects all CMMC levels to be achievable by its suppliers regardless of their size or other considerations (USDoD, 2020b). It is intended that this regime will be fully implemented across the USDoD's entire immediate and chain supplier base of some 300,000 organisations by 2025.

As discussed in Section 2.1, the NIST *Framework for Improving Critical Infrastructure Cybersecurity,* first introduced in 2013, was never a mandated framework but has since been widely adopted and accepted by companies and government agencies in many countries as

the de facto cybersecurity framework. Given the scale of the USDoD's CMMC deployment and the resources behind it, it is conceivable that its approach to cybersecurity assurance for the organisations it deals with could also become the de facto approach adopted by many other regulating bodies and the organisations they deal with across the globe. Certainly, if regulatory bodies do not feel the USDoD's approach is applicable for their cybersecurity regulation they should be required to explain why this is the case. Adoption of this compliance-based approach to cybersecurity would have far-reaching implications for companies and regulators who today adopt risk and principles-based methodologies.

6.1 Capability maturity models – a practitioner perspective

The view expressed by practitioners is that CMMs serve a useful purpose in developing a cybersecurity strategy but that their limitations must be clearly understood. This is evident from the comments of the divisional CISO of a European general insurance company who feels the picture presented by a CMM helps greatly in explaining what needs to be done and why, while also emphasising the steps the company must take to ensure the validity of the CMM process and outcome:

> *LM CISO:* CMMs have value but they need to be used with great caution and their limitations fully understood. We use a CMM to conduct internal benchmarking across the different businesses in our company. To ensure consistency of approach across our business units we have the process validated by an external party. We have been conducting this exercise for a number of years now. It is very easy to explain and helps ensure that what needs to be done gets done.

These sentiments are echoed by the group CISO of a global reinsurer, citing the benefit of using the ISF CMM internally to track progress over time but raising concerns regarding the validity of benchmarking against other organisations. He also notes that conducting the CMM process and the associated discussion can be very helpful in developing an organisation's cybersecurity knowledge and insights.

> *OL CISO:* The concern about the validity of using such CMMs for benchmarking with other organisations is very important. The real benefit of such tools is tracking your own performance over time. Many people are involved in answering the ISF control questions and we use expert judgement to determine our position on the scale. The discussion is very helpful.

An ISM refers to the importance of motivation if a CMM is to be used for benchmarking and specifically notes the dangers of the use of arithmetic means as employed in many CMMs.

The group CRO of a major life and pensions firm also raises concerns regarding motivation and how the output of a CMM can be used to the wrong end:

MS ISM: The motivation for conducting benchmarking is critical. Is an organisation trying to identify areas for improvement or to demonstrate it is at or above average and does not need to invest more in cybersecurity? Averages are deceptive.

CG CRO: The board and senior management focus on comparative maturity and that concerns me. It is useful to know if you are way behind but just because you are in front it doesn't mean you are where you need to be. This approach can be used to identify a weakness but not a strength.

Regarding the direction of cybersecurity regulation, the view of the practitioners was unanimous in thinking that the USDoD compliance-based approach using a CMM will become widespread within the next ten years at most, with some expressing the view that this regulatory approach is already with us in everything but name. The divisional CIO of a global bank notes that clients are already prescribing this as a requirement of the firm. The CRO of an asset management firm felt the use of CMMs by the regulator was particularly helpful as the motivation to ensure the accuracy of benchmarking data supplied to the regulator was likely to be high.

TOK CRO: While they do not acknowledge it explicitly, I feel that our regulators are using a CMM approach similar to the USDoD. I see this as a very useful benchmarking exercise as one can reasonably assume that when a company submits something to the regulator they are generally motivated to ensure it is correct and unambiguous.

CG CRO: Within 10 years the UK regulators will be mandating compliance in the same way the USDoD is proposing. It probably won't be as long as ten years. Already, the regulators are requiring firms to conduct a full-scale penetration test with findings reported to the regulator and the regulator providing prescriptive feedback based on the test outcome.

NS CIO: I can see Implementation of rigorously defined controls becoming the de facto approach adopted by regulators and I can see major clients imposing such requirements too. This is happening already.

While such a mandated approach may be more onerous for organisations, the idea was universally approved by the practitioners as it would help bring clarity to what cybersecurity measures are required of their organisations by regulators. And it would also help them in dealing with the big and growing challenge of cyber risk arising from third parties.

6.2 Capability maturity models – recommendation

Despite the limitations of CMMs, if consistently applied, they can be useful in tracking changes in an organisation's cybersecurity posture over time. The process of developing the input for a CMM and interpreting the output can itself be a very informative exercise. Effective benchmarking against external parties is very difficult because of inconsistencies in motivation and context. Such benchmarking may be helpful in identifying weaknesses but should never be used to draw comfort from apparent relative strength. Should regulators expand the use of CMMs this may make external benchmarking more reliable over time.

For organisations wishing to use a CMM, the model recommended here is the ISF as this currently appears to be the only facility with a readily available body of benchmarking data. With time, alternative CMMs used by regulators or other institutions may come to the fore.

7.0 PEOPLE AND PROCESS

A number of significant themes emerged from the industry practitioner research interviews. While all of these themes warrant elaboration in further works, it is felt that the importance placed on people and process by the industry practitioners necessitates immediate note. This point is highlighted by Verizon (2021) which reveals that 85% of all data breaches involve human interaction.

The emphasis of the interviewees on the importance of the board and senior executive in demonstrating ownership of the cybersecurity response was universal. The group CRO of a large asset management firm suggests that board members do not need to be cyber experts, but they do need to understand the issue and be able to engage with the regulator on the matter. The group CRO of a very large life and pensions business goes further, positing that every board in every industry must have members who understand cyber risk as well as the other traditional risks their organisation faces.

> *TOK CRO:* The board do not need to be infosec or cyber experts, but they do need to understand the subject and be able to explain it to the regulator if asked.

> *CG CRO:* Historically if you were on the board of an insurance company you needed to understand the investments you hold and the insurance you are writing. Now you need to understand cyber risk too. Asset risk, underwriting risk and cyber risk are the three things that can kill your business. An understanding of cyber risk now has to be a requirement for every board in every industry.

In addition to understanding cyber risk as well as more traditional risk categories, one ISE and an EA emphasise the need for boards and executives to understand that the dynamics of cyber risk have completely altered the timeframe for their decision-making.

> *MS ISM:* The topic is still quite new. I am sure that when other risks emerged it took quite some time for these to be understood. The problem is that the world is moving so fast today. Maybe twenty years ago you could take two years to make a decision, but the acceptable time now is two months because threats and technologies are changing so fast.

> *RT EA:* The new tools being developed for access control and security are good, but the speed of change is hard to keep up with. Access management today means something very different from access management 10 years ago.

The pace of change in cyberspace and the evolving threat landscape is such that the timespan available for decision-making regarding cybersecurity has collapsed when compared to how traditional risk types are approached.

While board engagement and support are essential for an effective cybersecurity programme this must be based on informed insight. Where this is not the case, inquiry from the board can become counterproductive as the group CISO of one firm noted. An EA commented that ill-informed boards can get distracted by the cybersecurity headlines of the day resulting in focus on the wrong issue, citing the increased emphasis on data encryption following the TalkTalk breach in 2015 as an example.

> *SE CISO:* We have all come across those board members who have learned just enough to ask what they think are clever questions but really they are just creating a lot of noise. It is important that boards challenge but they need to do so from an informed position.

> *RT EA:* The attack vector for TalkTalk was through the application layer. Having an encrypted database does not prevent the exfiltration of unencrypted data from this layer if a legitimate user's access has been hacked. There is a danger we are spending money on the wrong things driven by public and perceived regulatory expectations.

The need for senior executives of organisations to understand that security can never be assured was stated by the European ISM of an Asian-based global insurer, while the ISM of a UK-based life and pensions company spoke of the importance of the board understanding there is no path to steady "green".

MS ISM: Most senior executives are aware cyber risk is important but do not understand why. The simple principle that 100% security does not exist would be a good starting point. It feels like this is not understood.

DT ISM: Senior executives and the board need to understand there is no path to green as a steady-state. We will be constantly in and out of tolerance because of the rapidly changing external forces we are dealing with. The effort is relentless.

The same ISM emphasised the need for firms to recognise the difference between cybersecurity implementation plans being on track but the risk posture being out of tolerance:

DT ISM: It is important to differentiate between an organisation's plans being green and the actual risk posture. Plans may be green but our risk exposure may be red. The executive and the board need to understand this.

Many interviewees commented that effective technology is critical in managing cyber risk but that the implementation of technological solutions is rarely if ever optimum. Senior practitioners are critical of the tools and sales methods of cybersecurity vendors but also recognise that even the best technological solutions can be negated through error and omission by their organisations' people and process failures.

SE CISO: The effectiveness of some of the tools is questionable. We buy stuff from salespeople and don't even know if it works or works the way we expect it to. A lot of the time we are buying the wrong stuff.

LM CISO: There are too many tools not well implemented. And security product vendors provide a lot of hype. It is essential to get processes and controls in place first. A lot can be achieved with metrics and measuring. "A fool with a tool is still a fool".

MS ISM: In the end, it always comes back to people and processes. One can have the best technical measures in the world in place but if someone clicks on the wrong site or opens the wrong thing...

The need to ensure the work of the security team is monitored is reflected in the SANS (2021a) reporting of a White House memo providing advice to the private sector on protection from ransomware. The importance of checking the security team's work is emphasised. Understanding who watches the watchers is critical.

Given the importance of people and process in developing and maintaining a robust cybersecurity posture, the role of training, clear accountability and constant validation of controls is highlighted by the interviewees. The CRO of a global banking unit comments that his firm has an uncompromising approach to employee cybersecurity training. Missing cybersecurity training, even by a day, is considered to be a disciplinary offence.

> *CN CRO:* We don't mess about with training. It impacts compensation. A missed training deadline is considered a serious violation even if it is only missed by a day. There is no excuse.

As well as helping to build the organisation's cybersecurity knowledge base, this robust approach to training helps instil an organisation-wide cybersecurity culture. People understand this is a matter on which there needs to be no compromise. This security ethos needs to extend to software development and deployment where security by design becomes the norm and is embedded in the culture of these functions (NCSC, 2018d; Lopez et al., 2020). In addition, the divisional CISO of a European global insurer notes the importance of relentless monitoring of controls and ensuring clear accountability is in place.

> *LM CISO:* Day-to-day follow-up on controls is essential, as is having accountability across the end-to-end processing. Clear accountability is critical.

This point is reiterated by the ISM of a global Asian insurer. There can be no ambiguity about who in the organisation owns its data and other electronic assets, and who accepts the cyber risk these assets are subject to.

> *MS ISM:* In the end, it will always come down to who owns and accepts a risk. Absolute clarity on data ownership and who accepts the risks associated with this data is essential.

While technical solutions represent a critical component of any organisation's cybersecurity defences, the role of people and process are equally important. And the responsibility for ensuring both technical and organisational capabilities are fit for purpose sits with the board. Boards need to consider if they themselves have the capabilities required to operate in this new risk environment which requires a change in mindset concerning risk acceptance and speed of decision making, as well as new skills and knowledge. Even the very best cyber defence technical solutions will prove ineffective unless the people and processes supporting them are effective too. For this to happen, an uncompromising attitude to training, control monitoring and accountability are required.

8.0 PRACTICAL CONSIDERATIONS

This section presents key practical considerations for the development and implementation of a cybersecurity strategy as identified by the financial services practice head and a technical expert in a leading global cybersecurity advisory company. The findings of the literature review, output of the 14 practitioner interviews and the recommendations proposed in the report were shared with the two global implementation advisors (GIA), and a joint interview was held with them seeking their input on practical considerations that should be taken into account by organisations in developing a cybersecurity strategy and the implementation of the paper recommendations.

GIA: Make the strategy accessible using real-world threat scenarios.

Board and executive-level understanding of the cyber strategy and organisation's risk posture can be enhanced through the use of real-world threat scenarios.

As it may not be immediately apparent to the intended audience how the 1 to 5 scale mappings on the multiple dimensions of a risk assessment or CMM should be interpreted, the use of real-world scenarios can help make a cyber risk assessment and strategy more accessible for the board and executives. For this purpose, the meaningful cyber risk exposure of most companies is typically represented by five or so threat scenarios.

Assessing the implications for an organisation should any of these scenarios materialise - taking into consideration the effectiveness of the enterprise's controls, the changing threat landscape and the extent of its attack surface, including third parties - will help in establishing an understanding of the current risk posture and cyber strategy objectives.

Using threat scenarios to bring the strategy to life for the board and senior executive in this way can help ensure the funds required to implement and maintain the planned security capability are provided. Furthermore, "it can help manage the challenge of distracting questions from the board and senior executive arising from the cybersecurity news headlines of the day".

GIA: Do not underestimate the change management challenge. It is significant.

For the strategy to become a reality a clear roadmap identifying priorities, milestones, funding and other resources must be established. Given the clear and present danger represented by cyber risk most, if not all, organisations will have a desire to implement their cybersecurity strategy rapidly. Speed must not become the enemy of quality. Consideration must be given to how change at pace can be achieved without impacting the quality of execution.

GIA: Be aware and wary of bias.

In building a security capability for an organisation the CISO is typically both the customer and the supplier. Independent challenge is important to avoid bias and myopia. Also, beware the prioritisation of security initiatives determined by the discipline bias of decision makers and influencers such as the CISO, CRO and CIO.

GIA: Ownership of the implementation of a cyber strategy is fragmented.

The requirements of the security controls identified in the risk assessment for a cyber strategy often do not align with the responsibilities of one part of an organisation or another. Rather, the security effort is fragmented in nature with input required from multiple departments. Establishing ownership for the effective implementation of security controls can be an organisational challenge.

GIA: Board capabilities need to move beyond responding to updates.

Typically, the approach of boards and Executive Committees to cyber risk is to respond to a CISO's RAG report on an organisation's cybersecurity posture. However, boards and Executive Committees need to "understand the journey and not just be aware of the destination". In a rapidly changing environment, board and Executive Committees need to be aware of the challenges of getting to green, and if getting to stable green is a realistic objective?

***GIA*: Measuring and reporting cyber risk is a systemic challenge.**

Monitoring compliance to agreed controls is frequently used by organisations to assess the effectiveness of a cybersecurity programme. However, the understanding of how to measure and report cyber risk is a big and unresolved cybersecurity challenge today.

To be meaningful, cyber risk metrics need to articulate the threat exposure of an organisation to key performance indicators such as revenue and margin, and other critical factors such as reputation, all within the context of its risk posture. The use of real-world threat scenarios can help in identifying the right metrics.

***GIA*: CIS is a good place to start.**

In making sense of the alphabet soup, CIS is a good place to start. Mapping between NIST, CIS and ISF is feasible but it adds complexity. In the interest of simplification, organisations might consider basing their initial cybersecurity efforts on CIS alone. The extensive scope of the ISF control questions adds complexity and the value of benchmarking is limited, but if using ISF for any part of the process then use ISF for it all.

***GIA*: Quantifying cyber risk is desirable but hugely challenging.**

Limited data quantity and quality are things cybersecurity and ESG have in common.

While seeking to quantify the cyber risk an organisation faces is desirable, a paucity of good data makes quantifying cyber risk a real challenge.

***GIA*: Moving to the cloud can bring significant benefits. But it requires significant effort and brings new organisational challenges too. Today's IT and cybersecurity teams will see huge change over the coming years.**

Moving to the cloud can bring significant agility benefits to organisations and more and more companies will migrate to the cloud in pursuit of digital transformation for competitive advantage or, indeed, just to remain competitive. This migration will bring huge organisational change to traditional IT development, IT operations and cybersecurity teams. Much of the role of these functions will change from production and implementation to supplier assurance. This new focus requires a different skill-set and the transition of people from a role in a traditional "on-premises" IT operation to the cloud cannot be assumed.

Also, it must be understood that migration to the cloud is a huge undertaking that will take time and must be done with care if it is to avoid introducing new cyber vulnerabilities to a migrating organisation. A straight lift and shift of existing digital assets is not possible. Refactoring of existing applications must be undertaken to ensure they are cloud-ready and enabled with appropriate security controls.

The drive to digitization necessitates organisations to establish data links to third parties either as suppliers or customers, and this inevitably increases an organisation's attack surface. While dealing with third parties is unavoidable, organisations must seek to reduce any unnecessary complexity in their network, such as rationalising suppliers for example.

***GIA*: Some enterprises are seeking to create competitive advantage through their cybersecurity initiatives.**

Rather than view cybersecurity purely as a cost, some firms are considering how their cybersecurity efforts might be positioned as a value creator either through differentiation or the provision of security-based services. Clearly, such positioning can be helpful in obtaining funding for security initiatives.

However, the reality today is that the cybersecurity efforts of the vast majority of organisations are still nascent, and it will be some time before most are in any position to consider their cybersecurity capabilities in this context. This said, if an organisation can demonstrate a strong cybersecurity capability and record, this is a strength that could be deployed today to generate increased business from security-conscious customers and reduce costs, such as lower cyber insurance premiums for example.

Although the comments of the global advisory interviewees are largely consistent with those of the practitioners interviewed, of particular note are the emphasis of the advisors on the importance of making the cybersecurity strategy accessible through the use of real-world cyber threat scenarios, and not underestimating the magnitude of the organisation-wide effort required to implement such a strategy.

9.0 FUTURE TRENDS

While this section is intended to highlight some emerging trends in cyber risk and security anticipated by the industry practitioners interviewed and not covered elsewhere in the paper, the compressed time horizons of the cyber arena means that many of these "future" phenomenon are already upon us.

The use of technology in cyberattack and defence will increase as noted by the CRO of a large life and pensions company and the CISO of a major general insurer. The same CISO highlights the growing risk of machine-to-machine interaction and suggests that machine networks maybe 5 to 10 times larger than organisations think.

> *SE CISO:* The cloud can be very secure if it is configured properly. But activities need to be monitored.

> *CG CRO:* The use of quantum computing to hack encrypted data is a growing concern. And I can see artificial intelligence being used in both attack and defence.

> *SE CISO:* Continuous compliance will become more prevalent, facilitated by more automation.

> *SE CISO:* More and more security risk is machines talking to machines. What machines are on your network providing services for your organisation? There is growing evidence that there are a lot more machines linked to organisations' networks than expected – somewhere between 5 and 10 times more.

A range of positions are adopted by the subject matter experts on the use of cyber insurance: some choose to self-insure, others insuring some but not all business units based on risk and capital assessments, while a third group has extensive cyber insurance programmes in place. However, there is growing concern about the direction of the cyber insurance market, with some questioning if it will even be available in the future and, if so, will it be fit for purpose.

> *GH CISO:* I am quite fearful of where the cyber insurance landscape is going to go over the next two or three years. I think it will become incredibly difficult for organisations to get the cyber insurance needed to protect them from the risk they are facing. There will be riders in the policies that restrict the effectiveness of the policies. We are starting to get some claims history now and precedent is being set around some of the claims.

Intrinsically linked to cyber insurance is the rise of ransomware attacks: should ransoms be paid and, if so, should such payments be covered by insurance. As one Germany-based ISM observed:

> *MS ISM*: Some say the economics of ransomware crime is based on cyber insurance because insurers pay the ransom. I still think it is a good thing because insurance allows risk transfer.

The group CISO of a global payments company comments on the changing approach of some organisations and observes that the decision is not binary.

> *GH CISO:* Two or three years ago our position was not to pay ransoms – it was considered an inappropriate action and would make our organisation a target. However, we now feel this decision is not so binary and I think it would be an incredibly dangerous position for regulators to take the position that ransoms should not be paid. If, in the end, you can protect your company's reputation and even avoid harm to your customers by paying a ransom, why would that not be an appropriate approach?

Regardless of firms' views on the merits or otherwise of paying ransomware, this may ultimately be dictated to them by government authorities who are questioning the appropriateness of such payments. This is evident from the comments of some US government agencies following the Colonial pipeline attack (Politi, J. et al., 2021) and the decision already made by Axa, a global insurer based in France, to no longer offer cyber ransom insurance in France

following concerns expressed by the country's government officials (SANS, 2021b).

Another facet of cyber risk highlighted by many of the interviewees is the emergence of supply chains and other third-party relationships, including the cloud, as an attack vector. The view of the practitioners is that the oversight of such relationships as practiced today is not fit for purpose. There is a need to move from discrete auditing to continuous monitoring and businesses must do more to understand if the value of such third-party relationships justifies the increased cyber risk they bring. In response to these concerns some companies are actively reducing the number of third parties they engage with.

GH CISO: Historically, third-party risk assessments are largely compliance tick-box exercises. You go in once a year with a questionnaire and ask some questions. They swear they are doing it and you move on. This approach is not fit for purpose. Our desire is to move to more of a continuous monitoring model rather than an annual check. Over time I would even like to get to the point where we are using real-time telemetry inside their environments.

LM CISO: Understanding the security implications of multiple data centres in a hybrid environment – proprietary and public – is a huge challenge. What data is where? How do we meet our GDPR requirements? The service is very complex and this complexity and the associated risk warrants a reduction in the number of vendors.

NS CIO: We need to place much greater emphasis on the risk to our technology we are taking on with third parties. Does the financial reward really justify the risk?

OL CISO: Dealing with third parties is a big concern. And there is the issue of fourth parties whom our third parties deal with. Over the last two years we have been seeking to reduce the number of third and fourth parties we engage with. We are much more stringent.

As the CRO of a global bank points out, the concern about who you do business with is not limited to suppliers, it applies to customers too.

CN CRO: I can see a need for us to give greater consideration to cyber risk in our underwriting criteria for new clients. In gaining additional revenue, is there a possibility that we are taking on untoward cyber risk also?

Despite the importance of technological solutions, recognising the limitations of controls and the inevitability of cyber incidents happening, industry practitioners are calling on their organisations to place much greater emphasis on responding to and recovery from breaches by preparing incident response plans and conducting frequent firmwide rehearsals of these plans to build muscle memory.

SE CISO: Too much money is being spent by companies on the NIST prevent and detect domains and not enough on respond and recover. There are a lot of people who think if they invest enough money they will be safe and that is just wrong. Nobody is totally safe. Every CBEST test undertaken reveals problems. Every company can be breached. Once you accept that fact then you have to consider how to respond and recover.

GH CISO: Cyber preparedness is critical. To build muscle memory we have spent a lot of time doing real-time and live-fire simulation and tabletop exercises to create an extensive cyber response plan. I see a lot of companies that do not think about their level of preparedness. You can tell who has prepared and who hasn't prepared when you deal with them in a real crisis because it is clear if an organisation is making it up as it goes along or making decisions based on guidelines it has already created and tested. We conduct scenario testing with the CEO and Executive Committee every year. It is incredibly helpful.

It is evident from these comments that preparing and frequently practicing a cyber response plan is critically important. The difference between those organisations that have and have not done so

becomes very clear in a real crisis. The importance of such preparation cannot be overestimated. In the event of a breach under GDPR, regulators will consider the duty of care an organisation has shown for its data subjects such as customers and employees, and the steps taken by a firm to minimise the impact of a breach on those data subjects (Whitehead, 2019). Clearly such critical decisions are not something any organisation should be trying to determine in the middle of a cyber incident.

Continuing on the theme of the role that people play in facilitating cybercrime and defending against it, one CRO expressed concern at the amplified risk presented by the increasing interaction on social media between people's work and private lives and the resulting need for companies to understand what employees can and cannot say on social media. He also points out there is a declining tolerance in organisations for cyber infringements by employees. Another interviewee notes that the current approach to identity and access management is not fit for purpose and references the efforts of his company to establish a cyber risk score for all of its employees and contractors and use this in real-time decisioning for identity and access management.

> *CG CRO:* Social media is facilitating increasing interaction between people's work and private lives. It may be covered by the code of conduct but there is a need for companies to understand their rights in terms of what employees can and cannot say on social media. I feel there is a declining tolerance of cybersecurity infringements by employees such as repeated failing of phishing tests.

> *GH CISO:* The current approach to identity and access management is inadequate. Through our insider threat monitoring programme we collect over 80 attributes of behaviours and put this through a model to create an individual cyber risk score. Initially, this helped the cyber threat team to identify possible insider threat. But over time it will help us in our real-time decision-making around access provision.

These trends, which will have implications for employment law and employee relations, demonstrate the breadth of the effort that organisations need to consider in managing cybersecurity.

Defending against cyber threats is not just placing a financial burden on organisations, it also has a human cost. A number of the interviewees comment on the strain and potential burnout experienced by those charged with defending their organisations in the relentless cyber conflict. The tension causing this strain occurs at board and operational level.

> *SE CISO:* I know some CISOs whose boards go on two-hour training and then come back asking ridiculous questions that the CISO and her team have to deal with for months. It is as though you are not trusted to do your job and that can lead to a burned-out feeling. It can be frustrating.

> *GH CISO:* As I talk to other organisations, particularly non-financial services where the investment hasn't been made, I do see burnout.

> *NS CIO:* The technology people on the ground providing oversight and governance of controls have a tough job. They are charged with enforcing controls written by others that they often don't understand. And the cyber risk environment is changing so rapidly that the controls are changing constantly too. It is wearing for people to be in a constant state of conflict like this. If there is one thing I would like to fix it is this.

With the unrelenting battle against cyber threats set to remain with us for the foreseeable future, company boards and executives must ensure appropriate duty of care is shown to those employees who are engaged in the organisation's response to this perniciousness and may be impacted by the strain of the effort required.

10.0 CONCLUSION

Cyber threat is a very real, growing and potentially existential danger for every enterprise utilising any form of electronic data exchange, and organisations and their boards must take steps to address this challenge. This report identifies four broad categories under which an alphabet soup of frameworks and methods might be grouped in the development of a cybersecurity strategy: frameworks, fundamental controls, risk assessment and capability maturity models. From each of these four categories, which are populated by a vast array of artifacts, specific tools are recommended for use by organisations in the development of a cyber strategy:

- ***frameworks*** – adopt the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.
- ***fundamental controls*** – implement, as a priority, the six basic CIS controls and additional controls for malware defences, firewalls, data backups and secure remote access. These are recommended as the cybersecurity fundamental controls and are applicable to all organisations, from SMEs to MNEs.
- ***risk assessment*** – conduct an enterprise-specific qualitative risk assessment using CIS (RAM) or possibly ISF IRAM2, augmented where feasible by the FAIR Institute quantitative approach for organisations that have the necessary analytical capability. Subsequently, develop a plan to implement the risk treatments identified by CIS and ISF, which are NIST aligned. It is recommended that SMEs use only CIS which is more accessible than ISF.
- ***capability maturity models*** – use the ISF cybersecurity capability maturity model to monitor progress on the organisation's changing security posture over time and cautiously engage in external benchmarking. The use of CMMs and benchmarking is not recommended for SMEs.

The criteria on which these recommendations are made were determined from the literature review and research interviews:

- ***frameworks***
  - Widespread use/recognition
  - Constant updating/improvement
  - Acceptance by regulators
  - An effective level of detail
  - Accessible/understandable by range of stakeholders
- ***fundamental controls***
  - Universal minimum viable controls – applicable for an organisation of any size in any industry sector
  - Recommended by one or more national or supernational agencies
  - Balance of acceptable risk with resources and capabilities
- ***risk assessment***
  - Accessible/understandable by a range of stakeholders
  - Available data for quantitative methods
  - Allows triangulation with other methods
  - Fit with framework and controls
- ***capability maturity models***
  - Published models identified as being used by practitioners
  - Availability of benchmarking data

While addressing physical and electronic assets is essential, people and process are equally critical.

Future trends identified include the growth of risks arising from machine-to-machine interfaces, anticipated changes in cyber insurance, assessing the cyber risk associated with individual employees and the stress and burnout experienced by cybersecurity staff.

The task of addressing cyber risk is relentless and there is no such thing as 100 percent security, but there are practical steps that companies can and must take to help mitigate this highly dangerous and growing threat. This report, based on current literature and the experience of practitioners and advisors, provides managers with a recommended set of frameworks, standards and tools that they can adopt in seeking to protect their organisations' data subjects, such as employees and customers, as well as critical commercial data assets.

CITATIONS

Accenture (2019). *The Cost of Cybercrime. Ninth Annual Cost of Cybercrime Study.*

Available at: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

[Accessed last 21 May 2020]

ACSC (2020a). *Australian Government Information Security Manual.* Australian Government. Australia.

Available at: https://www.cyber.gov.au/sites/default/files/2020-08/Australian%20Government%20Information%20Security%20Manual%20%28August%202020%29.pdf

[Accessed last 17 August 2020]

ACSC (2020b). *Essential Eight to ISM Mapping.* Australian Government.

Available at: https://www.cyber.gov.au/sites/default/files/2020-06/PROTECT%20-%20Essential%20Eight%20to%20ISM%20Mapping%20%28June%202020%29.pdf

[Accessed last 25 September 2020]

Amutio, M., Candau, J. and Mañas, J.A. (2014). *MAGERIT—version 3.0: Methodology for Information Systems Risk Analysis and Management.* Ministry of Finance and Public Administration, Madrid, Spain.

Available at: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en

[Accessed last on 8 JUNE 2020]

Baig, A., Hall, B., Jenkins, P., Lamarre, E. and McCarthy, B. (2020). *The COVID-19 recovery will be digital: A plan for the first 90 days.* McKinsey Digital.

Available at: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-covid-19-recovery-will-be-digital-a-plan-for-the-first-90-days

[Accessed last on 2 June 2021]

Bourgeois, D. (2019). *Information Systems for Business and Beyond (2019).* The Open Text Book Challenge by the Saylor Academy.

Available at: https://opentextbook.site/informationsystems2019/

[Accessed last 8 May 2020]

BSI (2011). *BS ISO/IEC 27005:2011: Information technology.* Security techniques. Information security risk management (2011). British Standards Institute.

Available at: https://bsol-bsigroup-com.libezproxy.open.ac.uk/PdfViewer/Viewer?pid=000000000030228522

[Accessed last: 28 March 2021]

BSI (2015). *BS ISO/IEC 33001:2015 Information technology. Process assessment. Concepts and terminology.* BSI Standards Limited.

Available at: https://bsol-bsigroup-com.libezproxy.open.ac.uk/PdfViewer/Viewer?pid=000000000030241120

[Accessed last 31 October 2020]

BSI (2017). *BS 7799-3:2017: Information security management systems. Guidelines for information security risk management* (2017). British Standards Institute.

Available at: https://bsol-bsigroup-com.libezproxy.open.ac.uk/PdfViewer/Viewer?pid=000000000030354572

[Accessed last 14 August 2020]

BSI (2019). *BS ISO/IEC 33020:2019 Information technology. Process assessment. Process measurement framework for assessment of process capability.* BSI Standards Limited.

Available at: https://bsol-bsigroup-com.libezproxy.open.ac.uk/PdfViewer/Viewer?pid=000000000030396818

[Accessed last 30 October 2020]

BSI (2020). *IT-GrundschutzKompendium. Bundesamt für Sicherheit in der Informationstechnik.*

Available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.pdf?__blob=publicationFile&v=6

[Accessed last 15 October 2020]

Caralli, R.A., Stevens, J.F., Young, L.R. and Wilson, W.R. (2007). *Introducing octave allegro: Improving the information security risk assessment process* (No. CMU/SEI-2007-TR-012). Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst.

Available at: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

[Accessed last 28 July 2020]

Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J., Sweetnam, J. and Townsend, A. (2019). *[Project Description] Data Confidentiality: Detect, Respond to, and Recover from Data Breaches (Draft)* (pp. 13-13). National Institute of Standards and Technology.

Available at: https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/dc-drr-project-description-final.pdf

[Accessed last 14 May 2020]

CESG (2015). *Common Cyber Attacks: Reducing The Impact.* National Cybersecurity Centre.

Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf

[Accessed last 17 May 2020]

CINI (2019). *Framework Nazionale per la Cybersecurity e la Data Protection,* CIS-Sapienza Research Center of Cyber Intelligence and Information Security Sapienza Università di Roma e CINI Cybersecurity National Lab Consorzio Interuniversitario Nazionale per l'Informatica. Versione 2.0. Italia.

Available at: https://www.cybersecurityframework.it/sites/default/files/framework2/Framework_nazionale_cybersecurity_data_protection.pdf

[Accessed last 27 August 2020]

CIS (2018). *CIS RAM. Version 1.0 Centre for Internet Security Risk Assessment Methods.* Centre for Information Security.

Available at: https://learn.cisecurity.org/cis-ram

[Accessed last 26 May 2020]

CIS (2019). *CIS Controls V7.1.* Centre for Internet Security.

Available at: https://www.cisecurity.org/press-release/cis-introduces-v7-1-of-cis-controls-featuring-new-implementation-groups/

[Accessed last on 9 August 2020]

Clement, J. (2019). *Number of sent and received e-mails per day worldwide from 2017 to 2023.* Statista GmbH, Hamburg.

Available at: https://www.statista.com/statistics/456500/daily-number-of-e-mails-worldwide/

[Accessed last 16 May 2020]

Clement, J. (2020). *Annual number of data breaches and exposed records in the United States from 2005 to 2019.* Statista GmbH, Hamburg.

Available at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

[Accessed last 16 May 2020]

Council of the European Union, European Parliament (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).* Publications Office of the EU.

Available at: https://op.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en

[Accessed last 11 May 2020]

Cox, L., A. (2008). *What's Wrong with Risk Matrices?* Risk Analysis. Society for Risk Analysis.

Available at: https://inlac.org.ve/wp-content/uploads/2020/08/riskmatrices.pdf

[Accessed last 3 June 2021]

Crotty, J. (2019). *Some thoughts on the cybersecurity challenge – one INED's perspective.* ISACA Northern Chapter, Newcastle.

Available at: https://engage.isaca.org/northernenglandchapter/viewdocument/newcastle-event-available-slides?CommunityKey=6035adf3-99fb-46e6-9de6-d2d88d12a261&tab=librarydocuments&LibraryFolderKey=&DefaultView=folder

[Accessed last 12 May 2020]

DCMS (2020). *UK Cybersecurity Breaches Survey 2020.* Department for Digital, Culture, Media & Sport

Available at: https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020

[Accessed last 21 May 2020]

Deloitte (2107). *The Data Landscape. A Report for Facebook*.

Available at: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/technology-media-telecommunications/deloitte-uk-tmt-the-data-landscape.pdf

[Accessed last 5 May 2020]

Dhami, M.K., Mandel, D.R., Mellers, B.A. and Tetlock, P.E. (2015). *Improving Intelligence Analysis With Decision Science.* Perspectives on psychological science. SAGE Publications.

Available at: https://journals-sagepub-com.libezproxy.open.ac.uk/doi/pdf/10.1177/1745691615598511

[Accessed last on 8 August 2020]

ENISA (n.d.) *NIS Platform.* European Union Agency for Cybersecurity.

Available at: https://resilience.enisa.europa.eu/nis-platform#:~:text=The%20establishment%20of%20the%20NIS,Strategy%20of%20the%20European%20Union.&text=The%20NIS%20Platform%20will%20help,harmonised%20application%20across%20the%20EU.

[Accessed last 21 August 2020]

ENISA (2006). *Risk Management – Principles and Inventories for Risk Management / Risk Assessment methods and tools.* European Union Agency for Cybersecurity.

Available at: https://www.enisa.europa.eu/publications/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools

[Accessed last 24 July 2020]

ENISA (2016). *NCSS Good Practice Guide.* European Union Agency for Cybersecurity.

Available at: https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[Accessed last 27 August 2020]

ENISA (2018). *Cyber Europe 2018 – Get prepared for the next cyber crisis.* European Union Agency for Cybersecurity.

Available at: https://www.enisa.europa.eu/news/enisa-news/cyber-europe-2018-get-prepared-for-the-next-cyber-crisis

[Accessed last on 20 August 2020]

ENISA (2019). *ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends.* European Union Agency for Cybersecurity.

Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[Accessed last on 8 June 2021]

ENISA (2020a). *ENISA Threat Landscape: 15 Top in 2020.* European Union Agency for Cybersecurity.

Available at: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape-2020-top-15-threats

[Accessed last 7 June 2021]

ENISA (2020). *Top ten cyber hygiene tips for SMEs during covid-19 pandemic.* European Union Agency for Cybersecurity.

Available at: https://www.enisa.europa.eu/news/enisa-news/top-ten-cyber-hygiene-tips-for-smes-during-covid-19-pandemic

[Accessed last 25 September 2020]

European Commission, 2016. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Brussels.

Available at: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[Accessed last 27 August 2020]

Fafinski, S. and Minassian, N. (2009). UK Cybercrime Report.

FSB (2019). *Small firms suffer close to 10,000 cyber-attacks daily.*

Available at: https://www.fsb.org.uk/resources-page/small-firms-suffer-close-to-10-000-cyber-attacks-daily.html

[Accessed last 23 May 2020]

Foster, P., 2020. Cyber chief warns of east-west split over the internet. Financial Times.

Available at: https://www.ft.com/content/0aacf23f-0f71-4bdf-9ad3-5101ab80b259

[Accessed last 18 October 2020]

Freund, J. & Jones, J. (2015). *Measuring and managing information risk: a FAIR approach.* Butterworth-Heinemann.

GFS, 2018. Minimum Cybersecurity Standard. Government Security Group. UK.

Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/719067/25062018_Minimum_Cyber_Security_Standard_gov.uk__3_.pdf

[Accessed last 21 August 2020]

Gross, T. (2021). *Inner Workings Of DarkSide Cybergang Reveal It's Run Like Any Other Business*, Fresh Air.

Available at: https://www.npr.org/2021/06/10/1005093802/inner-workings-of-darkside-cybergang-reveal-its-run-like-any-other-business

[Accessed last 24 June 2020]

Heidt, E.T., Robins, A.E. & Tomhave, B.T. (2014). *Comparing Methodologies for IT Risk Assessment and Analysis.* Gartner Technical Professional Advice.

Heizenberg, J. (2018). *Watch These Data Analytics Challenges and Trends.* Gartner.

Available at: https://www.gartner.com/smarterwithgartner/watch-these-data-and-analytics-challenges-and-trends/

[Accessed last 6 May 2020]

Hilbert, M. & López, P. (2011). *The World's Technological Capacity to Store, Communicate, and Compute Information, Science.* United States: American Association for the Advancement of Science, 332(6025), pp. 60–65. doi: 10.1126/science.1200970.

Hippold, S. (2018). Build a Data-Driven Organisation, Gartner.

Available at: https://www.gartner.com/smarterwithgartner/build-a-data-driven-organization/

[Accessed last 2 June 2021]

Huadong, G., Wang, L., Chen, F. & Liang, D. (2014). *Scientific big data and Digital Earth.* Chinese Science Bulletin (Chinese Version). 59. 1047. 10.1360/972013-1054.

Available at: https://link.springer.com/article/10.1007/s11434-014-0645-3

[Accessed last 9 August 2021]

Hubbard, D. & Evans, D. (2010). Problems with scoring methods and ordinal scales in risk assessment. IBM Journal of Research and Development.

Available at: https://www.researchgate.net/publication/220498878_Problems_with_scoring_methods_and_ordinal_scales_in_risk_assessment

[Accessed last on 3 June 2021]

Hubbard, D.W. & Seiersen, R. (2016). How to measure anything in cybersecurity risk. Wiley and Sons.

Humphrey, W., Sweet, W.L., Edwards, R.K., LaCroix, G.R., Owens, M.F. and Schulz, H.P. (1987). *A Method for Assessing the Software Engineering Capability of Contractors.* Software Engineering Institute.

Available at: https://resources.sei.cmu.edu/asset_files/TechnicalReport/1988_005_001_15548.pdf

[Accessed last 3 November 2020]

IBM (2019). *Cost of a Data Breach Report 2019. Computer Fraud & Security.* Elsevier Ltd, 2019(8).

Available at: https://www-sciencedirect-com.libezproxy.open.ac.uk/science/article/pii/S1361372319300818

[Accessed last 21 May 2020]

IBM (2020). *Monte Carlo Simulation.* IBM Cloud Education.

Available at: https://www.ibm.com/cloud/learn/monte-carlo-simulation#:~:text= Monte%20Carlo%20Simulation%2C%20also%20known,outcomes%20of%20an%20uncertain%20event.

[Accessed last 3 June 2021]

ICO (n.d.). *Data security incident trends.* Information Commissioner's Office, London.

Available at: https://ico.org.uk/action-weve-taken/data-security-incident-trends/

[Accessed last 17 May 2020]

ICO (2018). *Guide to the Privacy and Electronic Communications Regulations.*

Available at: https://ico.org.uk/media/for-organisations/guide-to-pecr-2-4.pdf

[Accessed last 14 May 2020]

IDC & The Lisbon Council (2019). *D2.6 Second Interim Report, The European Data Market Monitoring Tool: Key Facts & Figures, First Policy Conclusions, Data Landscape and Quantified Stories.* IDC and the Lisbon Council.

Available at: http://datalandscape.eu/sites/default/files/report/D2.6_EDM_Second_Interim_Report_28.06.2019.pdf

[Accessed last 10 May 2020]

ISACA (2018). COBIT2019 Framework, Introduction and Methodology, ISACA.

Available at: https://community.mis.temple.edu/mis5203sec001sp2019/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodology_res_eng_1118.pdf

[Accessed last 14 August 2020]

ISF (2017). *Information Risk Assessment Methodology 2 (IRAM2) Suite.* Information Security Forum.

Available at: https://www.isflive.org/s/global-search/IRAM2

[Accessed last 10 August 2020]

ISO (2013a). *BS EN ISO/IEC 27001:2017: Information technology. Security techniques. Information security management systems. Requirements* (2013). British Standards Institute.

ISO (2013b). *BS EN ISO/IEC 27002:2017: Information technology. Security techniques. Code of practice for information security controls* (2013). British Standards Institute.

ISO (2018). *Standard No. 31000:2018: Risk management. Guidelines* (2018). International Organisation for Standardisation Technical Committee.

Kolini, F. & Janczewski, L. (2017). Clustering and Topic Modelling: A New Approach for Analysis of National Cybersecurity Strategies. PACIS 2017 Proceedings. 126.

Available at: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1160&context=pacis2017

[Accessed last on 27 August 2020]

KPMG (2019). *Fraud Barometer 2019: Commercialisation of cyber-crime.*

Available at: https://home.kpmg/uk/en/home/insights/2019/08/commercialisation-of-cyber-crime.html

[Accessed last 20 May 2020]

Kroese, D.P., Brereton, T., Taimre, T. and Botev, Z.I. (2014). *Why the Monte Carlo method is so important today.* Wiley Interdisciplinary Reviews: Computational Statistics. Wiley

Available at: https://people.smp.uq.edu.au/DirkKroese/ps/whyMCM_fin.pdf

[Accessed last 13 August 2020]

Krisper, M. (2021). Problems with Risk Matrices Using Ordinal Scales. Institute of Technical Informatics, Graz University of Technology.

Available at: https://arxiv.org/pdf/2103.05440.pdf

[Accessed last 3 June 2021]

Lam, J. (2017). *Implementing Enterprise Risk Management From Methods to Applications,* Wiley.

Mayer Brown (2018). *GDPR fines – lessons from competition law*, Legal Update December 2018, Mayer Brown.

Available at: https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2018/12/gdpr-fines---lessons-from-competition-law/files/updategdprfineslessonsfromcompetitionlawdec18/fileattachment/updategdprfineslessonsfromcompetitionlawdec18.pdf

[Accessed last 18 May 2021]

McGuire, M. Dowling S. (2013). *Cybercrime: a review of the evidence. Summary of key findings and implications.* Home Office, London,

Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf

[Accessed last 16 May 2020]

NCSC (n.d.). *About Cyber Essentials.* Cyber Essentials. National Cybersecurity Council.

Available at: https://www.ncsc.gov.uk/cyberessentials/overview

[Accessed last on 9 June 2021]

NCSC (2016a). *What is a cyber incident?* National Cybersecurity Centre.

Available at: https://www.ncsc.gov.uk/information/what-cyber-incident

[Accessed last 12 May 2020]

NCSC (2016b). NCSC Glossary. National Cybersecurity Centre.

Available at: https://www.ncsc.gov.uk/information/ncsc-glossary#:~:text=breach,in%20a%20non%2Dauthorised%20way.

[Accessed last 9 June 2021]

NCSC (2018a). *Small Business Guide: Cybersecurity.* National Cybersecurity Centre.

Available at: https://www.ncsc.gov.uk/collection/small-business-guide

[Accessed last 18 July 2021]

NCSC (2018b). *The fundamentals of risk.* National Cybersecurity Centre.

Available at: https://www.ncsc.gov.uk/collection/risk-management-collection/essential-topics/fundamentals

[Accessed last 4 August 2020]

NCSC (2018c). *Maturity models in cybersecurity: what's happening to the IAMM?* National Cybersecurity Centre.

Available at: https://www.ncsc.gov.uk/blog-post/maturity-models-cyber-security-whats-happening-iamm

[Accessed last 26 October 2020]

NCSC (2018d). *Secure development and deployment guidance*. National Cybersecurity Centre.

Available at: https://www.ncsc.gov.uk/collection/developers-collection

[Accessed last 24 June 2021]

NCSC (2019a). *Incident Management.* National Cybersecurity Centre.

Available at: https://www.ncsc.gov.uk/collection/incident-management

[Accessed last 21 August 2020].

NCSC (2019b). *NCSC CAF guidance.* National Cybersecurity Centre.

Available at: https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance

[Accessed last 21 August 2020]

NCSC (2021a). *New NCSC CEO warns against complacency while outlining future cyber risks.* National Cybersecurity Centre.

Available at: https://www.ncsc.gov.uk/news/ncsc-ceo-first-speech

[Accessed last 26 April 2021]

NCSC (2021b). *Cyber Essentials: Requirements for IT infrastructure.* National Cybersecurity Centre.

Available at: https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-2-2.pdf

[Accessed last 9 June 2021]

NCSC & NCA (2017). *The cyber threat to UK business 2016/2017 Report.*

Available at: https://www.ncsc.gov.uk/report/cyber-threat-uk-business

[Accessed last 23 May 2020]

Neely, L. (2016). *Exploits at the Endpoint: SANS 2016 Threat Landscape Survey.* SANS Institute.

Available at: https://www.sans.org/reading-room/whitepapers/firewalls/exploits-endpoint-2016-threat-landscape-survey-37157

[Accessed last 18 May 2020]

Netdiligence (2019). *Net Diligence Cyber Claims Study 2019 Report.*

Available at: https://netdiligence.com/2019/10/07/netdiligence-publishes-ninth-claims-study/

[Accessed last 21 May 2020]

NGMN Alliance (2015). *NGMN 5G White Paper.* A Deliverable by the NGMN Alliance.

Available at: https://www.ngmn.org/wp-content/uploads/NGMN_5G_White_Paper_V1_0.pdf

[Accessed last 10 May 2020]

NIST (2012). *NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems.* CreateSpace, Paramount, CA.

Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[Accessed last 8 June 2020]

NIST (2018). *Framework for Improving Critical Infrastructure Cybersecurity.* Version 1.1. National Institute of Standards and Technology.

Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[Accessed last 27 August 2020]

NIST (2019). *Developing Cyber Resilient Systems: A Systems Security Engineering Approach.* NIST Special Publication 800-160 Volume 2.

Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf

[Accessed last 3 June 2021]

NIST (2020a). *NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations.* National Institute for Standards and Technology.

Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[Accessed last 1 October 2020]

NIST (2020b). *Draft NIST Special Publication 800-53B, Control Baselines for Information Systems and Organizations.* National Institute for Standards and Technology.

Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B-draft.pdf

[Accessed last 1 October 2020]

Obama, B. (2013). *Executive order 13636: Improving critical infrastructure cybersecurity.* Federal Register. USA.

Available at: https://www.govinfo.gov/content/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[Accessed last 21 August 2020]

OECD (2013). *Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by "Big Data".* OECD Digital Economy Papers, No. 222, OECD Publishing, Paris.

Available at: http://dx.doi.org/10.1787/5k47zw3fcp43-en

[Accessed last 8 May 2020]

OECD (2017). "Types of cyber incidents and losses", in *Enhancing the Role of Insurance in Cyber Risk Management.* OECD Publishing, Paris.

Available at: https://read.oecd-ilibrary.org/finance-and-investment/enhancing-the-role-of-insurance-in-cyber-risk-management/types-of-cyber-incidents-and-losses_9789264282148-4-en#page1

[Accessed last 19 May 2020]

Open (2010). *Technical Guide FAIR – ISO/IEC 27005 Cookbook.*

https://publications.opengroup.org/downloadable/download/link/id/MC41NDM0OTIwMCAxNTk3NDMxNTQ0NjY1MTI3NjgyNzMzMTA4/

[Accessed last 14 August 2020]

Pergler, M. & Rasmussen, A. (2014). *Making better decisions about the risks of capital projects.* McKinsey on Finance, McKinsey & Company.

Available at: https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/corporate%20finance/mof/issue%2050/mof50_making_better_decisions.ashx

[Accessed last 5 August 2020]

Pfleeger, C. P., Pfleeger, S.L. & Margulies, J. (2015). *Security in computing.* Fifth edition. Pearson Education.

Politi, J., Manson, K., Brower, D., McCormick, M. and Murphy, H. (2021). *US opens debate over cyber ransom payments after pipeline hack.* Financial Times.

Available at: https://www.ft.com/content/ea2afceb-3770-414e-a14e-1238675fe63a

[Accessed last on: 15 May 2021]

PwC (2017). *Strengthening digital society against cyber shocks.*

Available at: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey/strengthening-digital-society-against-cyber-shocks.html

[Accessed last 23 May 2020]

Radicati (2019). *Email Statistics Report, 2015-2019.* The Radicati Group, Palo Alto.

Available at: https://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf

[Accessed last 16 May 2020]

Ralph, O. (2020). *Corporate cyber risk heightened by Covid,* warns ex-NSA head. Financial Times.

Available at: https://www.ft.com/content/57f59ed1-f3d7-4618-aed9-559a239177c1

[Accessed last 18 October 2020]

Rea-Guaman A.M., San Feliu T., Calvo-Manzano J.A., Sanchez-Garcia I.D. (2017a). *Comparative Study of Cybersecurity Capability Maturity Models.* In: Mas A., Mesquida A., O'Connor R., Rout T., Dorling A. (eds) Software Process Improvement and Capability Determination. SPICE 2017. Communications in Computer and Information Science, vol 770. Springer.

Rea-Guaman, A.M., Sánchez-García, I.D., San Feliu, T., Calvo-Manzano, J.A. (2017b). *Maturity models in cybersecurity: A systematic review.* 12th Iberian Conference on Information Systems and Technologies (CISTI). IEEE.

Available at: https://ieeexplore-ieee-org.libezproxy.open.ac.uk/stamp/stamp.jsp?tp=&arnumber=7975865&tag=1%5bAccessed last

[Accessed last 2 November 2020]

Reinsel, D., Ganz, J. & Ryding, J. (2018). *The Digitization of the World From Core to Edge.* International Data Corporation.

Available at: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

[Accessed last 5 May 2020]

Roser, M. & Ritchie, H. (2020). *Technological Progress.* OurWorldInData.org.

Available at: https://ourworldindata.org/technological-progress

[Accessed last 9 May 2020]

Roser, M., Ritchie, H. & Ortiz-Ospina, E. (2020). *Internet.* OurWorldInData.org.

Available at: https://ourworldindata.org/internet

[Accessed last 8 May 2020]

Safran (2021). *An Introduction to Qualitative Risk Analysis.* Safran.

Available at: https://www.safran.com/content/introduction-qualitative-risk-analysis#:~:text=Qualitative%20risk%20analysis%20involves%20identifying,either%20by%20source%20or%20effect

[Accessed last 3 June 2021]

Salkind, N. J. (2010). *Encyclopedia of Research Design.* Thousand Oaks: SAGE Publications.

Available at: http://sk.sagepub.com.libezproxy.open.ac.uk/reference/researchdesign/n469.xml

[Accessed last 23 May 2021]

SANS (2021a). White House Memo: *Advice to Private Sector on Protection from Ransomware.* SANS NewsBites Vol. 23 Num. 044. SANS NewsBites.

Available at: https://www.sans.org/newsletters/newsbites/xxiii-44/

[Accessed last on 10 June 2021]

SANS (2021b). *Insurer Will No Longer Reimburse Ransomware Payments in France.* SANS NewsBites Vol. 23 Num. 037. SANS NewsBites.

Available at: https://www.sans.org/newsletters/newsbites/xxiii-37/

[Accessed last on 15 May 2021]

Shackelford, S.J., Russell, S. and Haut, J. (2015). *Bottoms up: a comparison of voluntary cybersecurity frameworks.* UC Davis Business Law Journal.

Available at: https://heinonline-org.libezproxy.open.ac.uk/HOL/Page?collection=journals&handle=hein.journals/ucdbulj16&id=227&men_tab=srchresults

[Accessed last 24 August 2020]

SonicWall (2021). *SonicWall Cyber Threat Report.* SonicWall Inc.

Available at: https://media.bitpipe.com/io_15x/io_151295/item_2123742/2021-SonicWall-Cyber-Threat-Report%20%281%29.pdf

[Accessed last on 24 April 2021]

Standard Chartered (2017). *Cybercrime as a Service.*

Available at: https://av.sc.com/corp-en/content/docs/SCB_Fighting_Financial_Crime_Deep_dive_Cybercrime_as_a_Service_August_2017.pdf

[Accessed last 20 May 2020]

Symantec (2019). *ISTR Internet Security Threat Report.* Volume 24. Broadcom, San Jose.

Available at: https://docs.broadcom.com/doc/istr-24-2019-en [Accessed last 17 May 2020]

Sharot, T. (2011). *The optimism bias.* Current Biology, 21(23), pp.R941-R945. Elsevier.

Available at: https://www.sciencedirect.com/science/article/pii/S0960982211011912

[Accessed last on 7 August 2020]

Thelin, S. (2018). *Forecaster's Toolbox: How to Perform Monte Carlo Simulations.*

Available at: https://www.toptal.com/finance/financial-forecasting/monte-carlo-simulation

[Accessed last on 6 August 2020]

Thompson, E.L. & Smith, L.A. (2019). *Escape from model-land,* Economics, Volume 13, No. 1.

Available at: https://doi.org/10.5018/economics-ejournal.ja.2019-40

[Accessed last: 24 June 2021]

UK Companies Act (2006). Controller of Her Majesty's Stationary Office And Queen's Printer of Acts of Parliament.

Available at: https://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga_20060046_en.pdf

[Accessed last 9 June 2021]

USDoD (2020a). *Cybersecurity Maturity Model Certification (CMMC) CMMC Model v1.0 – Meeting Presentation.*

Available at: https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf

[Accessed last 31 December 2020]

USDoD (2020b). *Cybersecurity Maturity Model Certification (CMMC) Version 1.02*

Available at: https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf

[Accessed last 31 December 2020]

Verizon (2020). *2020 Data breach Investigations Report.*

Available at: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

[Accessed last 21 May 2020]

Verizon (2021). *Verizon 2021 Data Breach Investigations Report.* Verizon Communications Inc.

Available at: https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/summary-of-findings/

[Accessed last 16 May 2021]

Warrell, H. (2021). *Malicious software attacks 'spiralling out of control', report warns.* Financial Times.

Available at: https://www.ft.com/content/f3cc4243-5942-46d0-8d26-ee757c8f225f

[Accessed last on 24 April 2021]

Whitehead, M. (2019). *Customer Breach Support Duty of care: What does it mean in the context of a data breach under GDPR?* Perspectives. Deloitte LLP.

Available at: https://www2.deloitte.com/uk/en/pages/risk/articles/duty-of-care-what-does-it-mean-in-the-context-of-a-data-breach-under-gdpr.html

[Accessed last: 18 May 2021]

Williams, J. (n.d.). *OWASP Risk Rating Methodology.* OWASP.

Available at: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

[Accessed last 24 July 2020]

Yano, M., Penn, J.D., Konidaris, G. & Patera, A.T. (2012). *Math, Numerics & Programming (for Mechanical Engineers).* MIT.

Available at: https://ocw.mit.edu/courses/mechanical-engineering/2-086-numerical-computation-for-mechanical-engineers-fall-2012/readings/MIT2_086F12_notes_unit2.pdf

[Accessed last 6 August 2020]

APPENDIX

Research interview format, interviewees and data analysis methodology

A total of 16 cybersecurity and risk industry practitioners and advisors were interviewed remotely by video conference.

14 of the interviews were with industry practitioners and used a structured questionnaire to guide the discussion. A draft of the questionnaire was shared with the participants prior to the interview. With the approval of the interviewees, all of the interviews were recorded to facilitate subsequent analysis. While the scheduled time for the interviews was set at 45 minutes the actual time of all the interviews ranged from one to two hours. Consistent with the use of a reflective process for qualitative research, emphasis was placed on particular parts of the questionnaire as themes began to emerge and to reflect the expertise of individuals based on their roles.

While the majority of the practitioner interviewees were CISOs or CROs, the views of ISMs, a CIO, EA and global cybersecurity implementation advisors were also sought in order to gather a range of informed insight.

In addition to the 14 practitioners interviewed, a joint interview was held with the financial services cybersecurity practice head and a cybersecurity technical expert in a leading global advisory company. The findings of the literature review, output of the practitioner interviews and the recommendations proposed in the report were shared with the two global implementation advisors (GIA), and the joint interview sought their input on practical considerations that should be taken into account by organisations in developing a cybersecurity strategy and the implementation of the paper recommendations.

ROLE, REMIT AND GEOGRAPHIC RESPONSIBILITY OF INTERVIEWEES

Role	Remit	Global	Pan-European	Two or more countries	Single country
CISO[1]	Group	●			
CISO	Group	●			
CISO	Group			●	
CISO	Division[8]				●
ISM[2]	Group			●	
ISM	Group			●	
ISM	Division		●		
CRO[3]	Group				●
CRO	Group (deputy)			●	
CRO	Division		●		
CRO	Division		●		
CRO	Division			●	
CIO[4]	Division		●		
EA[5]	Group			●	
GIA PH[6]	Group	●			
GIA TE[7]	Group	●			

Notes

1 CISO: Chief Information Security Officer

2 ISM: Information Security Manager

3 CRO: Chief Risk Officer

4 CIO: Chief Information Officer

5 EA: Enterprise Architect

6 GIA PH: Global Implementation Advisor Practice Head

7 GIA TE: Global Implementation Advisor Technical Expert

8 All divisions are part of global organisations

Recording the interviews facilitated very close examination of the data and thematic analysis. While the interviewees offered a different area of focus or emphasis based on their role, clear and consistent themes emerged from the data analysis.

- Context and framework selection
- Reporting lines
- Line 1 or Line 2? Or Line 1.5?
- People and process are as important as the technology
- Facing up to reality – it is a business issue
- Learning to live with amber
- The threat from third parties
- Burnout
- The rise of the quants?
- To insure or not to insure?
- The direction of regulation – principles or compliance based?
- New threats and new responses

ABOUT THE AUTHORS

James Crotty

Independent Non-Executive Director and Adviser

Member of the International Advisory Board to The Open University Business School

Following a career of over two decades with American Express, James now holds a number of board and advisory roles across different sectors. Today, James is the chair of JPMorgan Wholesale Payments Europe; an independent non-executive director (INED) with Everest Re Ireland where he also chairs the risk committee; and sits on the board and the risk and audit committees of Aioi Nissay Dowa Europe. He has also served as an INED with the Swiss Re subsidiary, ReAssure.

At American Express, James held a number of senior international roles including Head of Customer Services, Europe and Head of Commercial Card, Europe. During this time, he also served as a member of the American Express European Governance Board and an advisor to the board of Amex (Saudi Arabia) Ltd. Before joining American Express James spent six years in the offshore oil industry.

In addition to his role as a member of the OUBS International Advisory Board, James has served the Stanford University Institute for Innovation in Developing Economies.

He has a BE from University College Cork, an MSc from University College London, an MBA from Manchester Business School and an MSc in Computing from the Open University. James is also a Certified Information Security Manager with ISACA.

Professor Elizabeth Daniel

Head of Department for Strategy and Marketing at The Open University Business School

Elizabeth is Professor of Information Management at The Open University Business School and is Head of Department for Strategy and Marketing. Her research focuses on the effective use of information systems by organisations and the individuals within them.

Her early research focused on large organisations including the NHS. She has produced many publications in leading academic journals and is joint author of the book *'Benefits Management: How to increase the business value of your IT projects'*.

More recently she has focused on IT in micro businesses and self-employment, with a particular interest in home-based businesses.

Prior to joining The Open University, Elizabeth was at Cranfield School of Management and City University Business School.

Before joining academia Elizabeth spent nearly 10 years in industry, including working as a management consultant undertaking strategic analysis and providing consultancy advice to a wide range of organisations.

ACKNOWLEDGEMENTS

The authors would like to thank the following colleagues from The Open University who reviewed this report:

Professor Arosha Bandara, Professor, School of Computing and Communications, Faculty of Science, Technology, Engineering & Mathematics

Dr Jon Hall, Entrepreneurial Academic and Practical Sage, School of Computing and Communications, Faculty of Science, Technology, Engineering & Mathematics

Professor Mark Fenton O'Creevy, Professor of Organisational Behaviour, The Open University Business School, The Faculty of Business and Law

With thanks to colleagues who helped to produce this report:

Astrid Alvarez, Senior Manager, Stakeholder and Alumni Engagement, The Faculty of Business and Law

Jacqui Thomasen, Head of External Engagement, The Faculty of Business and Law

TAKING IT FURTHER

Visit: **Business and Management short courses, modules and qualifications**
The Open University Business School: business-school.open.ac.uk/study

Short course with FutureLearn
Introduction to Cyber Security: futurelearn.com/courses/introduction-to-cyber-security

Modules or qualifications in Cyber Security
BSc (Honours) in Cyber Security: open.ac.uk/courses/computing-it/degrees/bsc-cyber-security-r60
MSc in Cyber Security: open.ac.uk/postgraduate/qualifications/f87